# TRANSPARENT, BALANCED AND VIGOROUS: THE EXERCISE OF THE AUSTRALIAN PRIVACY COMMISSIONER'S POWERS IN RELATION TO NATIONAL PRIVACY PRINCIPLE 4

**Jean Josephine Siganto**
**LLM**

Submitted in fulfilment of the requirements for the degree of
Doctor of Philosophy

Faculty of Law
Queensland University of Technology

April 2015

# Keywords

Security Principle

Information security best practice

National Privacy Principle 4

NPP 4

Australian Privacy Principle 11

APP 11

Privacy

Reasonable security

Responsive regulation

Principle-based regulation

# Abstract

Information security failures affecting the personal data held by Australian organisations are an issue of increasing concern. In Australia, one of the few legal obligations to secure personal data was contained in National Privacy Principle 4 (NPP 4) of the *Privacy Act 1988* (Cth) (now replaced by APP 11). NPP 4 required private sector organisations covered by the Act to 'take reasonable steps' to protect personal information. The Australian Privacy Commissioner ('the Commissioner') is given a broad range of powers by the *Privacy Act* to support compliance with NPP 4. The appropriate exercise of these powers in relation to NPP 4 should improve the security of personal information held by Australian organisations.

This thesis considers the extent to which the Commissioner's exercise of its powers in relation to NPP 4 could be regarded as an appropriate regulatory response to information security failures. The examination of the Commissioner's exercise of its powers is through a new conceptual framework which is in two parts. First, the exercise of powers is analysed by reference to an industry standard approach to information security. The second framework considers the exercise of regulatory power by reference to principles of transparency, balance and vigour. Transparency includes transparency of decision-making, which in turn introduces principles of procedural fairness, and transparency of compliance activities. Balance involves notions of proportionality and consistency and the targeted use of powers, while vigour refers to the frequency and timeliness of the Commissioner's use of powers.

The thesis is divided into three parts. Part 1 provides an analysis of information security practice to support the identification of an accepted industry practice approach to securing personal information. Consideration is also given to the implications for the Commissioner of the two regulatory models on which the *Privacy Act* is based: principle-based regulation and a responsive regulatory approach. This supports the identification of the second part of the conceptual framework, that regulatory powers should be exercised in a transparent, balanced and vigorous way. The Commissioner's broad range of powers is also considered, and divided into two groups: oversight powers and investigation powers. Part 2 examines the Commissioner's use of its oversight powers, including the provision of guidance,

education and advice. Part 3 examines the Commissioner's use of its investigation powers based on a detailed review of six NPP 4 own motion investigations conducted by the Commissioner, all of which related to high profile data breach cases.

Findings of the research include that, although there has been some improvement in general transparency and community engagement, it is difficult to characterise the exercise by the Commissioner of any of its oversight powers regarding NPP 4 as transparent, balanced or vigorous: there is no evidence of monitoring of non-compliance; where audits are conducted, the reports do not provide detailed guidance as to the Commissioner's interpretation of the Security Principle; there are few instances of the provision of advice or education relating directly to NPP 4 and only two guidance documents specifically covering NPP 4 have been released in 13 years. Similar findings are made in relation to the Commissioner's use of its investigation powers. All of the 6 investigations were conducted in response to media interest. In all of the cases, an "on the papers" investigation process was used, based on written responses to largely generic requests for information sent by the Commissioner to the six respondents, with little independent evidence gathering or confirmation of the facts as asserted by the respondents, whether directly or via third party investigation reports commissioned by the respondents. In each of the Commissioner's reports (other than Vodafone), the links between the Commissioner's understanding of NPP 4 (reflected in statements of general principle), the findings of fact, the stated reasons for decisions and the decisions themselves are unclear. The reports seem intended to provide community reassurance in response to media reports rather than real transparency of decision-making or guidance as to the Commissioner's interpretation and application of NPP 4 in different cases.

The Commissioner's use of powers also does not support an industry practice approach to information security. The OAIC's issued guidance does not explicitly use the risk based framework for the selection and management of security controls supported by most other sources of guidance on information security practice. The published investigation reports provide few connections between an industry practice approach to information security and the Commissioner's assessment of whether

reasonable steps had been taken. The investigation files suggest that the OAIC may not have a complete understanding of the intended operation of ISO 27001 and ISO 27002, the main international standards for information security. There is also evidence that the OAIC may not have the appropriate skilled resources to conduct investigations into data breach cases involving complex technical issues.

In conclusion, this thesis contends that the Commissioner's use of its powers in regard to NPP 4 has not been transparent, balanced or vigorous, nor has it been supportive of industry best practice. Accordingly, the Commissioner has not exercised its powers in the complex ways contemplated by the regulatory foundations of the *Privacy Act*. Until such time as it is able to do so, it is unlikely that the Commissioner's use of its powers in regard to the Security Principle will result in any significant improvement to the security of the personal information held by Australian organisations.

# Table of Contents

# List of Figures

# List of Tables

**Statement of Original Authorship**

The work contained in this thesis has not been previously submitted to meet requirements for an award at this or any other higher education institution. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made.

Signature: QUT Verified Signature

Date: April 2015

# Acknowledgements

Thank you to the long suffering Otto and to Dr Mark Burdon.  Your support has been invaluable.

# PART 1: BACKGROUND AND LITERATURE REVIEW

# Chapter 1: Introduction

## 1.1 BACKGROUND

Protecting personal information from unauthorised access, loss, misuse, or disclosure is an issue of increasing concern.[1]

A survey of data breaches in the first six months of 2014 reveals multiple incidents in which data, including names and addresses, credit card details and medical records, was accidently or inadvertently exposed to or compromised by attackers.[2] Many of these incidents, such as the Target attack that affected over 40

---

[1] In Nicole Brangwin, Foreign Affairs, Defence and Security, 'Cyber Security' (Research Publication, Parliamentary Library) < http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/BriefingBook44p/Cyber>, cyber security is referred to as a 'strategic priority for Australia's national security with the threat of cyber-attacks dramatically increasing.' Results from a survey by the Office of the Australian Information Commissioner show that a quarter (23%) were concerned about the risk of ID fraud and theft while 16% were concerned more generally by data security (16%) and the risks to financial data (11%).Office of the Australian Information Commissioner, 'Community Attitudes to Privacy Survey' 2013 <http://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf>).A survey completed in November 2012 involving over 1000 Australians aged between 18 and 65 found that 64% of respondents were concerned about the security of their online personal data while only 26% consider companies trustworthy of holding their data responsibly. *Australian Consumer Data Survey 2012* referred to in 'The 10 Worst Data Breaches of 2013' *ITBusinessEdge (online)* <http://www.itbusinessedge.com/slideshows/the-10-worst-data-breaches-of-2013.html>. Another survey of 4050 adults in 7 different countries found that 90% were concerned about data security. See, eg, Tom Pullar-Strecker, 'Leaked, Stolen Data Leaps', *Sydney Morning Herald* (online), 14 December 2012 <http://www.smh.com.au/it-pro/security-it/leaked-stolen-data-leaps-by-40-20121213-2bdhm.html>. Data security was the most common cause of complaint to the Australian Privacy Commissioner in 2008 – 2009 (Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2008 – 30 June 2009* (2009) 65 <http://www.oaic.gov.au/images/documents/migrated/2009-10-29012634/OPC_Annual_Report2008-09.pdf> ('*OPC 2009 Annual Report*')) and represented the cause of complaint in over 15% of cases in 2011 and 2012; see Office of the Australian Information Commissioner, *Annual Report 2010 - 2011* (2011) 37 <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201011/> ('*OAIC 2011 Annual Report*'); and Office of the Australian Information Commissioner, *Annual Report 2011 - 2012* (2012) 54 <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201112/> ('*OAIC 2012 Annual Report*').

[2] Martyn Williams, 'The 5 biggest data breaches of 2014 (so far)', *PC World* (online), 11 July 2014 <http://www.pcworld.com/article/2453400/the-biggest-data-breaches-of-2014-so-far.html>

million customers[3] and the eBay compromise that involved over 145 million members,[4] have received extensive international media coverage. In December 2012, the personal details of thousands of Australian military staff and students were stolen by a hacker who breached a university database at the Australian Defence Force Academy.[5] The stolen data, which included names, identification numbers, passwords, email addresses and dates of birth of about 10,000 students and 1,900 staff at the academy, was subsequently posted on several different websites.[6] Another successful attack affected a number of Australian online retailers, including the popular site 'Catch of the Day,' resulting in the loss of names, delivery addresses, email addresses, encrypted passwords and credit card data.[7]

The Australian Signal Directorate (ASD), which is responsible for advising the Australian Government on cyber security, believes that '[m]alicious cyber activity will continue to challenge Australia's national security, economic prosperity and

---

3 Brian Krebs, 'Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen', KrebsonSecurity, 10 January 2014 <http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/>; Grant Gross, 'Breach exposes data on 70 million customers, Target now says', *ComputerWorld* (Online), 10 January 2014 <http://cwonline.computerworld.com/t/8834412/980558529/651232/17/>; Michael Riley, Ben Elgin, Dune Lawrence, and Carol Matlack 'Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It', *Businessweek* (Online), 13 March 2014 <http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data>.

4 Denver Nicks, 'Investigators Target eBay Over Massive Data Breach', *Time* (Online), 23 May 2014 <http://time.com/110210/ebay-data-breach/>; Fran Foo, 'Warning after eBay passwords "stolen"', *The Australian* (online), 23 May 2014 <http://www.theaustralian.com.au/technology/warning-after-ebay-passwords-stolen/story-e6frgakx-1226927542280>; Brid-Aine Parnell, 'eBay faces Multiple Probes into mega-breach', *The Register* (online), 23 May 2014 <http://www.theregister.co.uk/2014/05/23/ebay_security_breach_investigations/>.

5 Markus Mannheim, '"It took three minutes": Defence data stolen in ADFA hack', *The Canberra Times* (online), 11 December 2012 <http://www.canberratimes.com.au/it-pro/security-it/it-took-three-minutes-defence-data-stolen-in-adfa-hack-20121211-2b6yp.htm>.

6 Ibid.

7 Josh Taylor, 'Catch of the Day waits 3 years to reveal data breach', *ZDNet* (online), 18 July 2014 < http://www.zdnet.com/au/catch-of-the-day-waits-3-years-to-reveal-data-breach-7000031759/>.

social wellbeing.'[8] The ASD points to four trends that are influencing this increase in malicious activity:

- Greater motivation to undertake cybercrime as more high-value information is stored and communicated on both government and commercial networks;
- Greater ability to acquire the skills to carry out cyber-attacks;
- Expansion of the spectrum of malicious actors; and
- Development of new technologies, particularly the growth in cloud computing, and the expanding use of mobile computing devices such as smartphones, laptops and tablet computers, which will increase the number of potential vulnerabilities.[9]

Despite growing concern about data breaches, whether caused by accident or malicious attack, and the impact that they may have on Australia's national security, economic prosperity and social wellbeing, it seems that a significant number of breaches could be prevented.

Many data breaches are the result of poor data security practices or of simple errors. Examples include sending letters containing medical information to the wrong people[10], or mistakenly publishing personal information online as a result of poor internal procedures. In February 2014, it was reported that the Australian Department of Immigration and Border Protection accidentally published the name, date of birth, country of origin, arrival date, and location of every asylum seeker in a mainland detention facility on the Department's website.[11] In March 2014, the

---

8 Australian Signals Directorate, *Information Security Manual Principles (September 2012 Release)* (Department of Defence, 2012) 6.

9 Ibid.

10 Adam Greenberg, 'St. Vincent Breast Center mails 63K letters to wrong people', *SCMagazine* (Online), 8 July 2014 < http://www.scmagazine.com/st-vincent-breast-center-mails-63k-letters-to-wrong-people/article/359791/>.

11 Allie Coyne and Paris Cowan, 'Immigration dept confirms asylum seeker data breach', *ITNews* (online), 19 February 2014 <http://www.itnews.com.au/News/372741,immigration-dept-admits-asylum-seeker-data-breach.aspx#ixzz366DGFeTf>, Jared Owens, 'Immigration admits asylum

National Tertiary Education Union contacted the Australia Privacy Commissioner after the details of over 2000 of its members at five universities were made public.[12]

The same poor security practices and simple errors that led to unintended disclosures of personal information also contribute to the success of malicious attacks. In its 2012 survey, Verizon reported that 96% of breaches resulted from attacks that were 'not highly difficult' and which could have been avoided through simple and inexpensive changes.[13] The most recent Verizon report notes that over 90% of all of the attacks considered by the reports over the last 10 years fall into one of only nine different 'attack patterns.'[14] This in turn suggests that information security incidents could be prevented if organisations implemented controls to mitigate only a small number of attacks.[15] This statistic is supported by the ASD, which reported that 85% of the attacks it responded to in 2011 'involved adversaries using unsophisticated techniques' that could have been prevented if the victims had

---

seeker privacy bungle: probe launched', *The Australian* (online), 19 February 2014 <http://www.theaustralian.com.au/national-affairs/immigration/immigration-admits-asylumseeker-privacy-bungle-probes-launched/story-fn9hm1gu-1226831518565>; Allie Coyne, 'Australia faces lawsuits over asylum seeker data breach', *ITNews* (online), 10 March 2014 <http://www.itnews.com.au/News/374603,australia-faces-lawsuits-over-asylum-seeker-data-breach.aspx>. Other reported incidents include Fran Foo, 'ACCC admits to data breach, but denies being hacked', *The Australian* (online), 11 April 2014 <http://www.theaustralian.com.au/technology/accc-admits-to-data-breach-but-denies-being-hacked/story-e6frgakx-1226881178192?nk=5a744d7d8b05049d7efbce9a1cf90d69>; Hedley Thomas and Emma Hart, 'CMC blunder exposes secret dossiers', *The Australian* (online), 6 March 2013 <http://www.theaustralian.com.au/national-affairs/state-politics/cmc-blunder-exposes-secret-dossiers/story-e6frgczx-1226591128641#>.

12 Julie Hare, 'Call to cops over privacy breach', *The Australian* (online), 5 March 2014 <http://www.theaustralian.com.au/news/call-to-cops-over-privacy-breach/story-e6frg6n6-1226845153676#>.

13 Verizon Ltd, *Data Breach Investigation Report* (2012). There are a number of other surveys that evidence the continuing problem of data being accessed by unauthorised third parties (both maliciously and accidently). See, eg, a survey by KPMG that reported that the amount of leaked or stolen data rose by 40%, including the loss of 6.5 million user passwords in July 2012 by social networking site LinkedIn, the loss of 1.5 million people's credit card details by financial services firm Global Payments and the loss by clothing retailer Zappos in January 2013 of the personal details including physical and email addresses of its 24 million customers. The report also said there had been no improvement in the security of information held by governmental and healthcare organisations. Reported in Tom Pullar-Strecker, above n 1.

14 Verizon Ltd, *Data Breach Investigation Report* (2014) 15.

15 Ibid.

implemented a package of four simple security safeguards.[16] More recently, a 2013 survey showed that attackers were still successfully exploiting well-known vulnerabilities that could be addressed by taking basic security measures.[17]

This failure to implement basic security protection is particularly concerning given the increase in targeted attacks, particularly those known as 'advanced persistent threats.'[18] If organisations are currently falling prey to attacks that could be thwarted by readily available and easy-to-implement security measures, they are even more likely to be unable to withstand a sophisticated, targeted, and continuous malicious attack.

National Privacy Principle 4 and its successor, Australian Privacy Principle 11 (APP 11), in the *Privacy Act 1988* (Cth), is one of the few legislative provisions regulating corporate information security practices in Australia.[19] NPP 4 (also known as the 'Security Principle')[20] required each private sector organisation

---

16 'At least 85% of the intrusions that ASD responded to in 2011 involved adversaries using unsophisticated techniques that would have been mitigated by implementing the Top 4 mitigation strategies as a package'; Australian Signals Directorate, *Top 4 Mitigation Strategies to Protect Your ICT System* (2012) <http://www.dsd.gov.au/publications/csocprotect/Top_4_Mitigations.pdf?&verNov12>.

17 Privacy Rights Clearinghouse, *Chronology of Data Breaches. Security Breaches 2005 - Present* (31 December 2013) <http://www.privacyrights.org/data-breach>.

18 For reports on targeted threats see, for example Pullar-Strecker, above n 1. For information on the nature of the cyber threats in 2013, and the more sophisticated attacks largely from organised criminal gangs see 'Global Payments Breach Tab: $94 Million', *DataBreach Today* (online) 10 January 2013 <http://www.databreachtoday.com/global-payments-breach-tab-94-million-a-5415?rf=2013-01-10-edbt&elq=b448ef0d32454de0ae87cd614dc3becc&elqCampaignId=5522>.

19 Other legislated security obligations include Rule 11.1(a) of *Privacy (Tax File Number) Rule 2015* (Cth), issued under the *Privacy Act* s 17, which requires Tax File Number ('TFN') recipients to take reasonable steps to safeguard TFN information. The *Personally Controllable Electron Health Records Act 2012* (Cth) ('PCEHR Act') requires that organisations participating in the Electronic Health Record System must take steps to secure data processed by that system. There are also a number of industry specific codes which include some security obligations. These include the *Code of Banking Practice* (Australian Bankers Association Inc, 2013) which is a voluntary industry scheme overseen by the Australian Bankers Association Inc. Another important code is the *Telecommunications Consumer Protections Code* (Communications Alliance Ltd, 2012) (in particular Clause 6.9).

20 In this research, where relevant 'Security Principle' means both NPP 4 and its successor Australian Privacy Principle 11 (APP 11).

covered by the Act[21] to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.'[22]

Ensuring that personal information is protected against unauthorised access, disclosure, modification, misuse, and loss is one of the basic principles recognised by most privacy regimes. The Fair Information Practice Principles,[23] the *OECD Privacy Guidelines*,[24] the *EU Directive on Privacy*,[25] and the APEC Privacy Framework[26] all contain a provision similar to NPP 4. Data security has been referred to as a 'constant theme' in all of the international instruments on data protection.[27] It was identified as one of the twelve fair information principles on which there was consensus by Bennett and Raab,[28] it is one of the basic principles applied by data

---

21 There are a number of exemptions and 'carve-ins' in terms of the private organisations covered by the *Privacy Act* There are a number of exemptions and 'carve-ins' in terms of the private organisations covered by the *Privacy Act*, for example, s6D(4) which provides that an organisation is not a 'small business' (and so will not come within the small business exemption from the Act) if it 'provides a health services to anther individual and holds any health information.' See also s7B(3) which exempts 'employee records' from the Act. These exemptions will not be discussed further in this research.

22 The National Privacy Principles were contained in *Privacy Act* Schedule 3. As of 12 March, 2014 the NPPs have been replaced by a new set of principles called the Australian Privacy Principles.

23 The Fair Information Practice Principles were originally proposed in the United States Department of Health, Education and Welfare's seminal 1973 report: Records, Computers and the Rights of Citizens, Report of the U.S. Secretary of Health, Education and Welfare's Advisory Committee on Automated Personal Data Systems, July, 1973 ('The HEW Report'). These principles are at the core of the Privacy Act of 1974, as amended, codified at 5 U.S.C. § 552a.

24 Organisation for Economic Cooperation and Development, *Guidelines Covering the Protection of Privacy and Transborder Data Flows of Personal Data* adopted by the OECD Council on 23 Sept. 1980 (OECD Doc. C(80)58/Final) ('*OECD Privacy Guidelines*'). Security Safeguards Principle 11, Part 2 of the *OECD Privacy Guidelines*.

25 *European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personla data and on the free movement of such data* [1995] OJ L 281/31, art 17.1.

26 Asia Pacific Economic Co-Operation Secretariat, 'APEC Privacy Framework' (2005) <http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/%2803995EABC73F94816C2AF4AA2645824B%29~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf> Principle 22 ('*APEC Privacy Framework*').

27 Rosemary Jay, *Data Protection Law and Practice* (Sweet & Maxwell, 4th ed, 2012) 305.

28 Colin J Bennett and Charles D I Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2nd revised ed, 2006).

processing laws referred to by Bygrave,[29] and it is one of the ten principles used by Greenleaf as a baseline for determining whether a data privacy law exists.[30]

Although the wording of the Security Principle differs between the different privacy regimes, the common, general requirement is that organisations must take 'reasonable care' to protect personal information. This general requirement is neither prescriptive nor precise. It articulates a substantive objective without providing any detail as to how that objective is to be achieved. This type of legal requirement is known as a principle.[31] The *Privacy Act* is an example of principle-based regulation: all of the main obligations pursuant to the Act (including NPP 4) were and are couched as general principles rather than prescriptive laws.

In any principle-based regulatory system, the regulator plays a pivotal role in ensuring that the regulated community understands what is required to achieve compliance with the principles. The Australian Privacy Commissioner ('the Commissioner') is the regulator responsible for ensuring compliance with the Security Principle, and as part of that role, establishing a common understanding regarding compliance. To assist the Commissioner as regulator in a principle-based system, it is given a range of powers. These powers fall into two main groups: oversight powers (including the ability to provide guidance, advice, and education, and to monitor and audit compliance) and enforcement powers (including the power to investigate potential interferences with privacy and make determinations).[32] These powers are intended to be used in a responsive manner.[33] This means that the

---

29 Lee Bygrave, *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002) 57.

30 Graham Greenleaf, 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) 23(1) *Journal of Law, Information & Science* 4, 11-12.

31 The difference between principles, bright line rules and complex or detailed rules is considered further in Chapter 2 below.

32 See, eg. the reference to the Commissioner's oversight and enforcement powers in Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice*, Report No 108 (2008), [45.10] ('*For your information'*).

33 The responsive regulatory approach and its relationship with the *Privacy Act* is considered in detail in Chapter 2.5.2.

oversight powers should be used in the first instance to ensure that the regulator's expectation of compliance is properly communicated. More punitive powers, which are associated with the use of the enforcement powers, should only be used in the case of serious or repeated infringements. The use of the oversight and enforcement powers in this hierarchical manner is consistent with a responsive regulatory approach (discussed further in Chapter 2). In view of the broad range of powers available to the Commissioner, it is important that those powers be used in the most appropriate way to ensure that the principles stated in the *Privacy Act* are met. When considering the exercise by the Privacy Commissioner of its powers, the Australian Law Reform Commission (ALRC) was of the view that the Commissioner should take a transparent, balanced, and vigorous approach to the use of the available powers to ensure compliance with the *Privacy Act*.[34]

Over the last 20 years, information security professionals have developed a broadly accepted approach to effective information security. Although there are variations, sufficient commonality exists among the main variants to support the proposition that, as a matter of industry practice, the accepted method to manage the security of information (and to reduce the risk of information security incidents) is by the use of a risk-based information security management system.[35] It would be expected that, in using its oversight and investigation powers to develop consensus on the compliance obligations imposed by NPP 4, the Commissioner would refer to this industry practice approach to information security. It would also be expected that the Commissioner would use the range of powers available in a transparent, balanced, and vigorous manner in order to build consensus, or, at the least, a common understanding, between the regulator and the regulated community regarding the Commissioner's interpretation of NPP 4 (consistent with an industry practice approach) and the Commissioner's application of that interpretation in different circumstances.[36]

---

34 *For your information,* above n 32, [4.74].

35 The industry best practice approach to information security is discussed further in Chapter 3.4 below.

36 *For your information,* above n 32, [4.35]. The relationship between these principles and accepted principles for the exercise of regulatory powers is discussed further in Chapter 2.6.

The relationship between the appropriate use of regulatory powers (based on the principles of transparency, balance, and vigour) and industry practice to support the desired outcome of 'reasonable' protection of personal data held by Australian organisations is represented by *Figure 1*. The transparent, balanced, and vigorous use of the Commissioner's available power should support the adoption of industry-accepted information security practices to produce the outcome of a reasonable level of protection of the personal information held by Australian organisations.

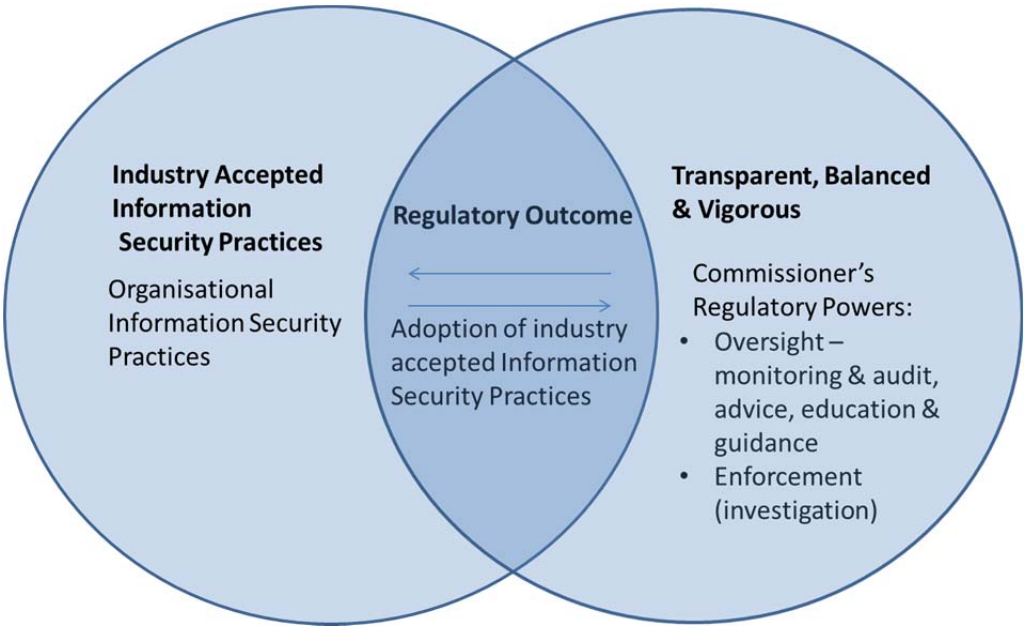



*Figure 1: Framework to assess what is an appropriate regulatory response to NPP 4.*

This thesis will examine the Commissioner's exercise of its oversight and investigation powers in relation to NPP 4. In doing this, the thesis will address a question of increasing importance to Australian corporations and the general community.

If the Commissioner's exercise of regulatory powers in relation to NPP 4 involves the transparent, balanced and vigorous consideration and application of 'reasonable' security measures assessed by reference to accepted industry information security practices, there will be greater certainty as to what security measures Australian corporations need to take in order to meet their NPP 4

compliance obligations. As a consequence, the personal information of Australians should be more appropriately protected.

## 1.2 RESEARCH QUESTION

The key research question of the thesis is:

*To what extent is the exercise of the Commissioner's investigation and oversight powers in relation to NPP 4 an appropriate regulatory response?*

This research question gives rise to three sub-questions. They are:

1. What oversight and investigation powers are available to the Privacy Commissioner?
2. What is the relationship, if any, between the exercise of those powers and recognised industry practice in Australia?
3. To what extent is the exercise of those powers consistent with principles for the exercise of regulatory powers?

## 1.3 THESIS STRUCTURE

The research question posed by this research is answered in the following parts.

Part 1 (Chapters 1 to 4) includes a literature review, a consideration of the two regulatory systems that are the foundations of the Act (principle-based regulation and a compliance approach), and an outline of the conceptual framework to be used as the basis of the analysis of powers included in Parts 2 and 3. The conceptual framework includes two elements: the extent to which the exercise of the investigation and oversight powers by the Commissioner could be regarded as transparent, balanced, and vigorous; and the extent to which the Commissioner's interpretation of reasonable steps for the purposes of NPP 4 is consistent with an industry approach to information security.

Part 2 (Chapters 5 and 6) contains an analysis of the Commissioner's use of its oversight powers in regard to NPP 4. Chapter 5 reviews the Commissioner's monitoring, audit, advice, and education powers, and analyses the use of those powers with reference to the two components of the conceptual framework. The Commissioner's use of its guidance powers is considered separately in Chapter 6.

This includes the guidance documents that have been issued, together with case notes and pre-February 2011 own motion investigation reports (OMI reports) that involved any consideration of NPP 4. Again, the use of the guidance power is considered through the lens of the conceptual framework used in this research.

Part 3 (Chapters 7 to 10) analyses the Commissioner's investigation powers. To date, enforcement of compliance with the *Privacy Act* by the Commissioner has principally involved the investigation of complaints and the conduct of Commissioner-initiated investigations, called own motion investigations (OMI). The Commissioner has the power to make determinations, which power is considered in Chapter 7. However, the power has been used infrequently and rarely in regard to NPP 4. Accordingly, this research will focus on the use of the investigation power. The Commissioner's published guidance on its approach to the use of its investigation powers is considered in Chapter 7. To support the analysis of how the Commissioner has conducted its investigations, a group of 6 OMI reports published between February 2011 and July 2012 has been selected for detailed consideration. These cases are introduced in Chapter 8, which describes the factual details and the findings made in each of the published reports. Chapter 9 analyses each of the 6 investigations, using the framework of the transparent, balanced, and vigorous use of powers, to determine the extent to which these investigations could be regarded as consistent with principles for the exercise of regulatory powers. Chapter 10 examines each investigation by using the framework of industry practice to determine whether the investigations and resulting reports could be regarded as supporting an industry practice approach to 'reasonable steps' to secure personal information.

Chapter 11 summarises the findings from this research, applies the findings to answer the research questions, and concludes with a short consideration of the implication of the findings from this research for the future.

## 1.4 LIMITATIONS OF RESEARCH

This research is limited to the consideration of NPP 4 of the *Privacy Act*.

A separate privacy principle, Information Privacy Principle 4 (IPP 4), formerly applied to government agencies. This principle was different from NPP 4.[37] It obliged government agencies to take steps to prevent the unauthorised use or disclosure of personal information that had been disclosed to a third party in connection with the provision of a service to the agency. IPP 4 had no provision equivalent to the obligation to destroy information pursuant to NPP 4.2 In view of these differences; this research is confined to the consideration of information security incidents affecting the private sector only.

This research is further confined to consideration of:

- Those private sector organisations that fall within the operation of the *Privacy Act*. There are significant exemptions from the operation of the *Privacy Act*, including the exemption for 'small business;'[38] and
- 'Personal Information' as defined in the Act.[39] Although defined broadly enough to cover, for example, the collection of information by health service providers, there are significant areas where the Act has no application, for example, in the protection of corporate confidential information or trade secrets. 'Employee records' held by private organisations are also exempt from the operation of the Act.[40] The consideration of information other than 'personal information' as defined in the *Privacy Act* is outside the scope of this research.

This research commenced in 2010 and is concerned with the exercise of powers by the Commissioner. Accordingly, this research will consider the *Privacy Act* as it was

---

37 *Privacy Act* Schedule 2 Information Privacy Principle 4.

38 *Privacy Act* s 6. Small businesses are those with an annual turnover of $3 million or less. For guidance on the meaning of 'small business' for the purposes of the *Privacy Act*, see http://www.privacy.gov.au/business/small/guidance

39 *Privacy Act* s 6(1) defined personal information as "... information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion." This has been amended effective 12 March 2014. This amendment is not material for the purposes of this research.

40 Ibid s 7B(3).

before the amendments introduced by the *Privacy Amendment Act*[41] became effective, although reference is made to amendments wherever relevant. However, it is noted that there are few substantive differences between NPP 4 and APP 11,[42] and accordingly the findings of this research should continue to have some relevance post March 2014. Consideration of the implications of this research in the context of the amended Act is included in the concluding chapter of this research.

The Commissioner's use of its powers is ongoing. However, this research needed to limit its scope in point of time. Accordingly, it includes detailed consideration of instances of the exercise by the Commissioner of its powers in relation to NPP 4 up to March 2014 only. Audits completed and determinations and guidance issued after March 2014 are outside the scope of this research. The consideration of the Commissioner's use of its investigation powers in Part 3 relied on data collected regarding the investigations. To enable the collection and analysis of relevant data, consideration of OMI Reports is limited to those issued up to March 2013 only. This limitation is discussed further in Chapter 4 below.

## 1.5 RELATIONSHIP OF RESEARCH TO PUBLISHED RESEARCH

The review of the literature relevant to the question raised by this research can be considered by reference to the following:

- Literature relating generally to the legal obligations of Australian corporations to secure information;
- Literature relating to NPP 4 as part of the *Privacy Act*; and
- Literature relating to the exercise of powers by the Commissioner to support compliance with the Act.

---

41 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth) ('*Privacy Amendment Act*').

42 See Chapter 2.3 for more detailed consideration of the differences between NPP 4 and APP 11.

### 1.5.1 Information Security and Australian Law

The increased media interest and public concern in response to the growing number of information security incidents involving personal information might be expected to be reflected in the literature.

Unfortunately in Australia there has is little recent legal literature regarding the regulation of information security practices.[43]

Only one recent Australian legal text considers legal issues associated with securing information and the consequences of failing to adequately secure information.[44] Although this text does not undertake a detailed analysis of NPP 4, it does consider the meaning of 'reasonable security' noting that, although it might be assumed by non-experts that there is a universal 'benchmark' against which the adequacy of a security regime may be assessed, it is not, in reality, straightforward because of the 'relative' nature of the security and its relationship with the management of risk.[45] It recommends that organisations adopt a standards-based information security management system to meet various obligations to provide reasonable security.[46] The legal obligation to keep information secure is considered by another, more recent Australian text, which notes the *Privacy Act* principles and the problem for the Commissioner in providing guidance that may rapidly become outdated through swift technological change.[47] The text also refers to industry standards such as ISO 27001[48] and ISO 27002,[49] and PCI DSS,[50] suggesting that

---

43 An Australian based academic has authored a number of articles relating to information security liability – including one of the standard of care. However, these are set in the context of the laws of the United States, not Australia. See for example De Villiers, M., Information Security Standards and Liability. 2010 Journal of Internet Law 13.

44 Nick Gifford, *Information security: managing the legal risks* (CCH Australia Limited, 2009).

45 Ibid Chapter 12.

46 Ibid 193 – 194.

47 Margaret Jackson and Marita Shelly, *Electronic Information and the Law* (Lawbook Co, 2012) 127 – 132.

48 International Standards Organisation, *ISO/IEC:27001:2013 Information technology – Security techniques – Information security management systems- Requirements* (2013) ('*ISO 27001*').

49 International Standards Organisation, *ISO/IEC 27002:2013 Information technology – Security Techniques – Code of Practice for Information Security Management* (2013) ('*ISO 27002*').

'[a]dherence to an approved standard can be used as a defence against claims of negligence.'[51] These references to industry standards as the basis for considering what is reasonable security are pertinent to the discussion in Chapter 3 of the industry practice approach to information security, and the use of that approach as part of the conceptual framework for considering the Commissioner's exercise of powers.

The regulation of information security in Australia has been considered from the perspective of a proposed data breach notification law, which concludes that these notification laws are unlikely to lead to better information security.[52] The article does not refer to the obligation to take reasonable steps in NPP 4 or to the use by the Privacy Commissioner of its powers to support organisational compliance with NPP 4.

### 1.5.2 NPP 4

To date, there have been no cases in Australia where a court has considered what might constitute 'reasonable steps' to protect personal information for the purposes of NPP 4.

In the absence of binding legal decisions, the Office of the Privacy Commissioner (OPC) and the Office of the Australian Information Commissioner (OAIC)[53] have published case notes and own motion investigation reports (OMI reports) that provide some guidance about how the Commissioner has interpreted and applied NPP 4 in different cases. These case notes and OMI reports and the principles which can be derived from them, together with the guidance issued by the

---

50 Payment Card Council, 'Payment Card Industry Data Security Standard v3.0' <https://www.pcisecuritystandards.org/security_standards/> ('PCI DSS').

51 Jackson and Shelly, above n 47, 127 – 132.

52 Sara M Smyth, 'Does Australia Really Need Data Breach Notification Laws - And If So, What Kind' (2012-2103) 22(2) *Journal of Law, Information and Science* 159.

53 The Office of the Privacy Commissioner ('OPC') became part of the Office of the Australian Information Commissioner ('OAIC') in 2010, after which time case notes and own motion investigation reports were published by the OAIC rather than the OPC.

OAIC that explains the OAIC's interpretation of NPP 4 and the way the Commissioner conducts investigations, are discussed in later chapters.

There are a large number of texts which cover Australian privacy laws. These texts refer to the inclusion of NPP 4 in the legislation but devote little discussion to the meaning or intended or actual operation of that principle.[54] For example, in the consideration of NPP 4 in *Annotated National Privacy Principles*, reference is made to the Commissioner's published guidelines and the factors indicated as relevant to determining what is reasonable in those guidelines.[55] In terms of meeting the requirements of NPP 4, the text recommends a compliance strategy based on the implementation of policies designed to address issues identified by an information security risk assessment, together with compliance with an industry standard (a similar approach to that recommended by the information security legal texts discussed).[56]

IPP 4 (the equivalent of NPP 4 which applied to public entities) and NPP 4 were examined as part of a University of New South Wales Interpreting Privacy Principles Project in 2006.[57] The research made the point that information security is a separate and mature area of expertise. It referred to the deference shown by privacy regulators to the established expertise of the information security industry and the consequent tendency of those regulators (including the then OPC) to refer to general standards and guidelines on security, rather than to be overly prescriptive regarding what was required by the Security Principle.[58] The research did however caution that care should be taken when using generic information security standards

---

54 See, eg, Carolyn Doyle and Mirko Bagaric, *Privacy Law in Australia* (Federation Press, 2005), Margaret Jackson, *Hughes on Data Protection in Australia* (Lawbook Co, 2nd ed, 2001), and Jeremy Douglas-Stewart, *Annotated National Privacy Principles* (Presidian, 2009).

55 Douglas-Stewart, above n 54, [2-2950] - [ 2-3252].

56 Ibid [2-30307].

57 Nigel Waters, Graham Greenleaf and Paul Roth, 'Interpreting the Security Principle' (2006) <http://www.cyberlawcentre.org/ipp/publications.html; Waters, Nigel, 'Interpreting the Security Principle' (Paper presented at Symposium: Interpreting Privacy Principles: Chaos or Consistency?, Sydney, 17 May 2006), Nigel Waters and Graham Greenleaf, 'IPPs examined: The Security Principle' (2004) 11(3) *Privacy Law & Policy Reporter* 67.

58 See, eg, *Interpreting the Security Principle*, above n 57, 8 – 10.

in the context of protecting personal information. In particular, it suggested that those standards may not necessarily address unauthorised access by authorised personnel or limitations on the collection of personal information.[59] The research also noted the importance of risk in determining what is 'reasonable.'[60] It suggested that a number of general principles relevant to NPP 4 can be derived from the Commissioner's guidance and case notes. These included, for example, that given the number of disclosures that relate to 'human error', the importance of appropriate training and enforcement (which is part of 'personnel security') is clear.[61] Similarly, the project supported the proposition that the existence of access controls and an audit facility is an important part of taking reasonable security measures.[62] The work did not seek to compare the Commissioner's interpretation of NPP 4 to industry practice, nor did it consider the extent to which the exercise of powers in relation to NPP 4 can be considered as in accordance with principles of good regulation.

The Commissioner's application of NPP 4 in the context of the Sony data breach and the *Guide to Information Security: 'Reasonable Steps' to Protect Personal Information*[63] (*Guide to Information Security*) has been considered in a more recent article which is covered in more detail later in this research.[64]

Otherwise, there has been little detailed consideration of NPP 4 in the literature.

---

59 Ibid.

60 Ibid 6.

61 Ibid 13-14.

62 Ibid 11-13, 21 – 22.. Subsequent case notes have supported this proposition, for example, *N v Utility Provider* [2006] PrivCmrA 13; *M v Commonwealth Agency* [2008] PrivCmrA 13; but compare *FH v NSW Department of Corrective Services* [2003] NSWADT 72.

63 Office of the Australian Information Commissioner, *Guide to Information Security: reasonable steps to protect personal information* (2013) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-information-security> ('*Guide to Information Security*').

64 Geoff Bloom and Kristina Frketic, 'The OAIC's new Guide to Information Security, the hacking of 77 million Sony users, and the privacy breach that cost $171 million' (2013) 9(9) *Privacy Law Bulletin* 150. The Commissioner's data breach investigations were also reviewed in Andrew Miers and Elise Martin, 'Lessons from recent data breaches' (2012) (9) 2 Privacy Law Bulletin 24.

### 1.5.3 Commissioner's Exercise of Powers

More literature relates to the functions and powers of the Privacy Commissioner and the way that those functions and powers have been used. This was a topic of particular interest at the time of the two most recent ALRC reviews on the introduction of the new amendments.[65] More recently, there has been some consideration of the Commissioner's investigation into the Google Street view incident which, among other things, notes the absence of transparency in decision-making in the statements made by the Commissioner about that investigation.[66] There has also been some consideration of the new powers that came into effect in

---

[65] See, eg, Lee A Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law - Part 1' (2000) 7(1) *Privacy Law and Policy Reporter* 11; Lee A Bygrave, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law - Part 2' (2000) 7(2) *Privacy Law and Policy Reporter* 3; Graham Greenleaf, 'The "Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24(1) *University of New South Wales Law Journal* 262; Graham Greenleaf, Nigel Waters and Lee A. Bygrave, 'Promoting and enforcing privacy principles:an analysis of ALRC proposals for the role of the Privacy Commissioner' (Cyberspace Law and Policy Centre, 2007) <http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Enforce_final.pdf>, Nigel Waters, Abi Paramaguru and Anna Johnston, 'Enforcement of privacy laws – issues arising from Australian experience v.2' (Working Paper No 3, Cyberspace Law & Policy Centre, UNSW, November 2007). Graham Greenleaf, 'Reforming reporting of privacy cases: A proposal for improving accountability of Asia-Pacific Privacy Commissioners' in Paul Roth (ed), *Privacy Law And Policy In New Zealand* (LexisNexis Butterworths, 2003) ('*Reforming reporting of privacy cases*'); Graham Greenleaf and Nigel Waters, 'Australia's Privacy Bill 2012: Weaker Principles, Stronger Enforcement' (2012) 118 *Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012* 16 ('*Weaker Principles*'); Anthony Bendall, 'The governance of privacy : speak softly and carry a big stick' (2009) 60 *Australian Institute of Administrative Law National Forum* 39; Graham Greenleaf and Nigel Waters, '"Making privacy law safe for business": Australia's 2012 privacy Bill' (2012) 8(10) *Privacy Law Bulletin* 266 ('*Making Privacy Law Safe*'); Mark Hummerston, 'Sword or Shield: The Role of a Regulator' (Paper presented at Interpreting Privacy Principles Symposium, University of New South Wales, 3 June 2007) <http://www.cyberlawcentre.org/ipp/events/symposium07/Sword%20or%20shield.pdf>; Kevin O'Connor, 'The Federal Privacy Commissioner : pursuing a systemic approach' (2001 ) 7(1) *University of New South Wales Law Journal Forum* 13.

[66] Mark Burdon and Alissa McKillop, 'The Google Stree View Wi-Fi Scandal and its Repercussios for Privacy Regulation' (2014) 39(3) *Monash University Law Review* 702.

March 2012,[67] including the potential issues for the Commissioner in the enforcement of new APP 8.[68]

There has been little consideration of the way the Commissioner has elected to use its powers specifically in relation to NPP 4, apart from the work undertaken as part of the University of New South Wales project[69] and the 2008 ALRC review.[70] Specifically, there is no research into the use by the Commissioner of its oversight or investigation powers in relation to either NPP 4 or information security incidents more generally.

There also appears to be only limited research into the operation and enforcement of the equivalent of the Security Principle in other jurisdictions with similar regimes for the protection of personal information to that in Australia.[71] There has been more consideration by legal scholars in the United States regarding how the Federal Trade Commissioners have responded to information security

---

67 Ashley Tsacalos and Vanessa Verzi, 'Civil penalties for breach of privacy — coming soon!' (2013) 10(2) *Privacy Law Bulletin* 28; Charles Alexander, Elisabeth Koster and Helen Paterson, 'Punitive powers guided by ambiguity: the Australian Federal Privacy Commissioner's new powers in the context of a principles-based privacy regime' (2013) 9(5) *Privacy Law Bulletin* 66.

68 John Dieckmann, 'The new APP 8: crack down on cross-board data flows' (2012) 8(10) *Privacy Law Bulletin* 270.

69 See Waters, Greenleaf and Roth, above n 57; and Waters and Greenleaf, above n 57.

70 See Australian Law Reform Commission, 'Review of Privacy Issues Paper 31' (2006) <http://www.alrc.gov.au/ip-31>, which asked generally whether the Privacy Commissioner's powers to oversee the *Privacy Act* are appropriate and exercised effectively.

71 See, eg, Martin Meints, 'The Relationship between Data Protection Legislation and Information Security Related Standards' in Vashek Matyáš et al (eds), *The Future of Identity in the Information Society: IFIP Advances in Information and Communication Technology* (Springer Boston, 2009) 254; Andrew Charlesworth, 'The future of UK data protection regulation' (2006) 11(1) *Information Security Technical Report* 46, Jeff Langenderfer and Don Lloyd Cook, 'Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance' (2004) 57(7) *Journal of Business Research* 734; John Woulds, 'Information privacy and security - A regulator's priorities' (1997) 2(1) *Information Security Technical Report* 38. There has been some review of the operation of the equivalent of the *Privacy Act* in other jurisdictions. In the UK, the Rand Report reviewed the effectiveness of the Data Protection Act - See Neil Robinson et al, 'Review of the European Data Protection Directive' (RAND Coporation, 2009). In Canada there is a five year review regime in place, supporting the release of the 2008 Privacy Commissioner Report 'Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)' (Office of the Privacy Commissioner of Canada, 2008).

incidents, although that study was from the perspective of protecting consumers from unfair and deceptive practices, and in the context of a regime that does not have comprehensive data protection laws similar to the *Privacy Act*.[72] There has also been significant attention paid to the data breach notification laws passed by various states of the US, which laws could be regarded as a regulatory response to information security incidents.[73] However, given the different regulatory approaches to securing personal information taken in Australia and the United States, the US literature regarding the operation of data breach notification laws has limited relevance.

## 1.6 INFORMATION SECURITY AND PRIVACY

Given the focus of this research on the operation of the Security Principle within the Australian privacy regime, it is worth considering how information security has been viewed in the privacy literature.

*Figure 2* below represents the relationship between the objectives of information security (discussed in more detail in Chapter 3) and the main objectives of most current data protection laws.

---

72 See, eg, T D Breaux, and D L Baumer, 'Legally 'reasonable' security requirements: A 10-year FTC retrospective' (2011) 30(4) *Computers & Security* 178; A Serwin, 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption of Best Practices' (2011) 48 *San Diego L. Rev* 809, J L Henry et al, 'FTC Proposes Broad New Privacy Framework, and Asks "How It Might Apply in the Real World"' (21 December 2010) *K & L Gates* < http://www.klgates.com/ftc-proposes-broad-new-privacy-framework-and-asks-how-it-might-apply-in-the-real-world-12-21-2010/> , J S H Hiller, and D L Baumer, 'Due Diligence on the Run: Business Lessons Derived from FTC Actions to Enforce Core Security Principles' (2009) 45 *Idaho Law Review* 35; and M D Scott, 'The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?' (2008) 60 *Admin. L. Rev*. 129.

73 Some of the literature relating to data breach notification laws in the United States includes S A Needles, 'The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law' (2009) 88 *N.C.L. Rev* 267; K Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law'(2006) 75(1) *Fordham Law Review* 355; S Romanosky, D A Hoffman, and A Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) 11(1) *Journal of Empirical Legal Studies* 74; S Romanosky, R Telang, and A Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) *Journal of Policy Analysis and Management* 256; J W Schneider, 'Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data' (2009) 15 *Boston University Journal of Science & Technology Law* 25; P M Schwartz and E Janger, 'Notification of Data Security Breaches' (2007) 105(5) *Michigan Law Review* 913.

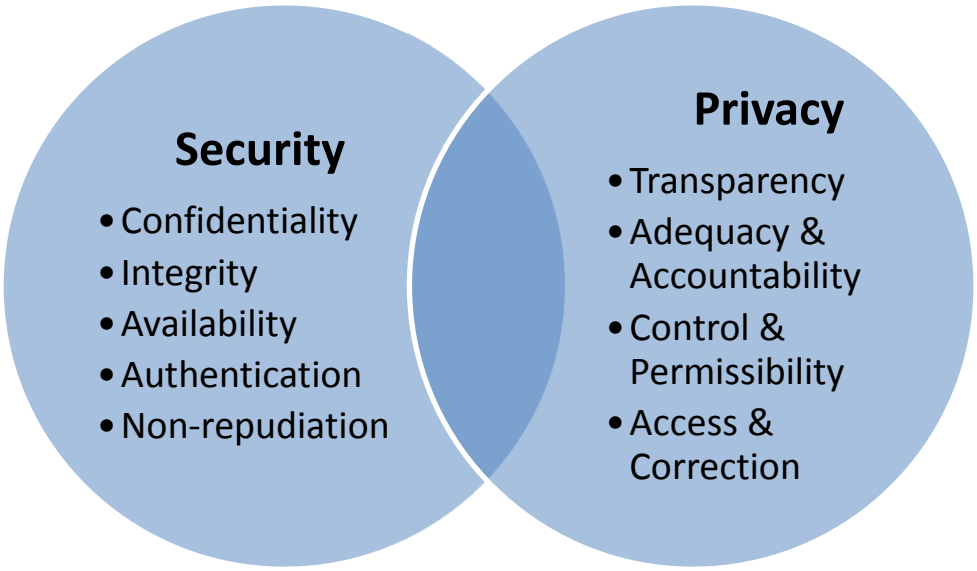



*Figure 2: Relationship between information security and privacy*

Although considerable overlap exists between the two, the objectives of information security are different to those of privacy.[74] While information security is an important part of privacy, information security does not exist solely to protect personal information. Equally, privacy concerns more than the protection of personal information from specified harms.

The distinction between privacy and security has perhaps been most explicitly recognised in the context of computer design, with information security design focusing on useability, while privacy design considers issues such as consent and control.[75] By contrast, within the privacy literature, information security has been viewed as an enabler of privacy, rather than an objective in its own right.[76] One

---

74 Ann Cavoukian and Mark Chanliaj, 'Privacy and Security by Design: A convergence of paradigms' (Information and Privacy Commissioner, Canada, 2013) <http://www.privacybydesign.ca/content/uploads/2013/01/pbd-convergenceofparadigms.pdf>.

75 See, eg, P Dourish and K Anderson, 'Collective information practice: exploring privacy and security as social and cultural phenomena.' (2006) 21(3) *Human-computer Interaction* 319; Kenneth Radke, '"Who decides?": security and privacy in the wild'(Paper presented at the 25th Australian Computer-Human Interaction Conference: Augmentation, Appluication, Innovation, Collaboration, 2013).

76 Sam DeKay and Ken Belva, 'Privacy Roles and Responsibilities' in Warren Axelrod, Jennifer Bayuk, and Daniel Schulzer (eds), *Enterprise Information and Security* (Artech House 2009) 9; 'The role of information security is to implement the mechanisms that establish and enforce

American commentator has stated that concern for individual privacy is '[p]erhaps the biggest driver of laws requiring security.'[77] Of course, some commentators have recognised information security and privacy as overlapping, but not totally congruent, notions.[78] The explanatory material attached to the *OECD Privacy Guidelines* notes that 'security and privacy issues are not identical.'[79]

However, the distinctions between privacy and security and the implications of those distinctions for the regulation of privacy and information security do not seem to have been explored rigorously or systematically. The tendency of the privacy literature to conflate security and privacy could be regarded as obscuring these distinctions.[80] A recent article has pointed to at least one important consequence of this conflation.[81] According to the author, privacy establishes a normative framework for deciding who should legitimately have the capability to access and alter information, whereas security implements those choices via a set of mechanisms.[82] The author suggested that a security failure is different to the

---

privacy rights'; and 13 'History reveals privacy is the 'why' and information security is the 'how'.' Similarly, Jane Strachan in 'Cybersecurity Obligations' (2005) 20 Me. B. J. 90, seems to assume that information security is the protection of personal information. She concludes that 'Information security is a key component of information privacy'.

77 Thomas J Smedinghoff, *Information Security Law : The Emerging Standard for Corporate Compliance* (IT Governance Publishing, 2008) 49.

78 Dean William Harvey and Amy White, 'The Impact of Computer Security Regulation on American Companies' (2002) 8 *Texas Wesleyan Law Review* 505, 508 points out that it is important to distinguish 'privacy' as involving 'the right of individuals to control the use and disclosure of information about them' and 'security' as meaning the 'safeguards ... to protect information from unauthorised access, attacks from outside the organisation, and from misuse and negligence with the organisation.' See also Calvin C Gotlieb, 'Privacy: A Concept Whose Time Has Come and Gone' in D Lyon and E Zureik (eds), Surveillance, Computers and Privacy (University of Minnesota Press, 1995); Paul Thompson, 'Privacy, Secrecy and Security' (2001) 3(3) *Ethics and Information Technology* 13. See also Lukas Feiler, *Information Security Law in the EU and the U.S.: A Risk-Based Assessment of Implicit and Explicit Regulatory Policies* (A Joint Initiative of Stanford Law School and the University of Vienna School of Law, 2011) 71 <http://www.law.stanford.edu/program/centers/ttlf/papers/feiler_wp9.pdf>.

79 Explanatory Memorandum, OECD Privacy Guidelines <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum > 56.

80 See references at n **Error! Bookmark not defined.**

81 Derek E Bambauer, 'Privacy Versus Security' (2013) 103(3) *Journal of Criminal Law and Criminology* 667.

82 Ibid.

balancing of opposing interests and rights implicit in consideration of the right to privacy, and that we should be less forgiving of security failures than of privacy failures.[83] His argument was that there are no competing moral claims to resolve in information security failures and that they make all parties worse off. As a consequence, the author supported a clear distinction in enforcement approaches between privacy and security breaches. The analysis of information security as largely mechanistic is consistent with the industry standard approach to information security put forward in this research. The proposition that the regulatory model that is best for privacy may not be as appropriate for the regulation of information security is relevant to this research. If it is the case that the Commissioner's exercise of powers is not "appropriate" based on the conceptual framework used in this research, it may be that the regulatory models that underpin the Privacy Act and which inform the way that the Commissioner's powers should be exercised are not the best models for ensuring the information is properly secured.

## 1.7 CONCLUSION

The number and severity of data breach incidents continues to highlight the problem of ensuring that information is appropriately protected.

The Security Principle is one of the few statutory provisions in Australia that requires organisations covered by the *Privacy Act* to take reasonable steps to protect personal information from misuse, loss, or unauthorised access or disclosure. This requirement makes the Security Principle an important regulation in regard to organisational information security practices.

NPP 4 was framed as a principle. Accordingly, its meaning and application should be established by the regulator responsible for ensuring compliance with the principle. It might be expected that, in establishing its understanding of NPP 4, the Privacy Commissioner as the relevant regulator would exercise the wide range of powers it has available, including both oversight and investigation powers, to support the adoption of steps that are commensurate with an accepted industry practice

---

[83] Ibid 669.

approach to information security in order to protect personal information. If that were the case, then NPP 4 would be applied in an appropriate way to support the protection of the personal information of Australians.

To date, information security has received limited consideration in the Australian legal literature. When it has been considered, the concept of 'reasonable security' has been couched in the context of industry standard approaches, such as those of *ISO 27001* and *ISO 27002*. Similarly, there has been little recent consideration of NPP 4, either in its own right or by reference to the Commissioner's use of its powers to support an interpretation or application of NPP 4.

By examining in detail the Australian Privacy Commissioner's exercise of powers in relation to NPP 4, through the lens of industry best practice and of the transparent, balanced, and vigorous use of powers, the research results from this thesis will fill an important gap in the privacy law literature. They may also influence the future use by the Commissioner of its powers to ensure that the personal information of Australians is properly protected.

# Chapter 2: The Commissioner's Powers

This chapter will briefly trace the development of privacy laws before examining in more detail NPP 4 as part of the Australian privacy regime. It will then consider the functions and powers given to the Australian Privacy Commissioner, pursuant to the *Privacy Act* in the context of the regulatory foundations for the *Privacy Act,* which are:

- Principle-based regulation or PBR; and
- A responsive approach to enforcement.

The current literature will be reviewed to identify the implications of these two regulatory foundations for both the regulator and for the regulated community.

The analysis in this chapter will answer the first sub-question in this research: What powers are available to the Privacy Commissioner pursuant to the *Privacy Act* in relation to information security failures? The principles for the exercise of regulatory powers will provide that part of the conceptual framework used to answer the third sub-question in this research: To what extent is the exercise of the Commissioner's powers consistent with principles for the exercise of regulatory powers?

## 2.1 BACKGROUND AND LITERATURE REVIEW

In the 1960s, the increasing use of computers around the world by both public and private entities raised considerable public concern about information privacy.[84]

[84] Gehan Gunasekara, 'Paddling in unison or just paddling? International trends in reforming information privacy law' (2014) 22(2) *International Journal of Law and Information Technology* 141, 143. See also Priscilla M Regan, *Legislating Privacy: Technology, Social Values and Public Policy* (University of North Carolina Press, 1995).

Commentators devoted significant attention to the issue[85] with privacy becoming an important public policy item in the US and other jurisdictions.[86]

For example, in the UK, the Younger Committee was commissioned to consider computing in the private sector in 1972, concluding that 'the computer problem as it affects privacy in Great Britain is one of apprehensions and fears and not so far one of facts and figures.'[87] Only four years later in 1976, a second committee recognised that the increasing general use of computers was a concern and recommended the passage of legislation that later became the first UK *Data Protection Act*.[88] In the United States, public concern about the US Social Science Research Centre proposal to establish a Federal Data Centre to provide access to and coordinate the use of government statistical information resulted in a report commissioned by the Secretary of Health, Education and Welfare and released in 1973 (the *HEW Report).*[89] The *HEW Report* recommended that Congress enact legislation adopting a *Code of Fair Information Practices* for automated personal data systems (operated by both the public and private sectors). The Code set out a list of rights that individual 'data subjects' (people whose personal information was stored) should have, and made specific recommendations for laws that would implement and enforce this Code. One of those recommendations required organisations that were keeping automated databases on individuals to enact

---

85 Daniel Solove, 'A Brief History of Information Privacy Law' (Public Law Research Paper No 215, George Washington University Law School, 2006) [1-24]. Solove refers to the following in support of this statement: Alan Westin 'Privacy and Freedom' (1967), Arthur Miller 'The Attack on Privacy' (1971); 'Nomos X11: Privacy' (J Ronald Pennock & J W Chapman eds. 1971); Alan Westin & Michael A. Baker 'Databanks in a Free Society' Computers Recordkeeping and Privacy' (1972); Kenneth L. Karst, 'The Files': Legal Controls Over the Accuracy and Accessibility of Stored Personal Data, 31 L. & CONTEMP. PROBS. 342 (1966); Symposium, Computers, Data Banks, and Individual Privacy, 53 MINN. L. REV. 211–45 (1968); Symposium, Privacy, 31 L. & CONTEMP. PROBS. 251–435 (1966).

86 Priscilla Regan, 'Privacy and Commercial Use of Personal Data: Policy Developments in the United States' (2003) 11(1) *Journal of Contingencies and Crisis Management* 1; Regan, above n 83.

87 Report of the Committee on Privacy, Cmnd. 5012, HMSO,1972.

88 Report on the Committee of Data Protection (1978) Cmnd 7341.

89 The HEW Report, above n 23.

safeguards to protect this data. This requirement was a precursor of NPP 4.[90] Many scholars believe that the *Code of Fair Information Practices* has influenced the development of privacy law in the United States and around the world.[91]

The *Code of Fair Information Practices* from the *HEW Report* was incorporated into the US *Privacy Act of 1974*,[92] as were additional, more prescriptive provisions specific to ensuring data security. The Act required agencies to 'establish appropriate administrative, technical and physical safeguards to ensure security and confidentiality of records to protect against any anticipated threats or hazards.' This model of dual recognition of computer security and the protection of privacy included in the U.S. *Privacy Act* has continued in the range of sector-specific laws that have been passed in the United States.[93]

These sector-specific laws in the US support a broadly similar approach to information security, that is, that there should be a documented security management process in place that involves the identification and analysis of risks and the implementation of a range of administrative, physical and technical safeguards that reduce risks and vulnerabilities to a reasonable and appropriate level.[94] This legislative approach to information security in the US is consistent with the industry practice approach to information security discussed in Chapter 3.

---

90 Principle 5 of the Fair Information Principles, above n 23. The five core principles of privacy protection recognised by the Code are: (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5) Enforcement/Redress.

91 Regan, above n 85, 14; Marc Rotenberg, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' (2011) *STAN. TECH. L. REV.* 1

92 *Privacy Act* of 1974, 5 U.S.C. § 552a

93 The U.S. sector specific laws include for example *Health Insurance Portability and Accountability Act*, 42 U.S.C. 1320d-2 and 1320d-4 (HIPAA) and Final HIPAA Security Regulations, 45 C.F.R. Part 164 and Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805

94 This commonality of requirements in regard to information security has led some commentators to suggest that in the U.S. there is a general duty of care in regard to securing data. See, eg, Smedinghoff, above n 77.

In Australia, concerns regarding privacy and increasing computerisation were first raised in 1973.[95] The Law Reform Commission produced two reports considering the issue: the first in 1979, which focused on issues relating to the 1976 Census,[96] and the second in 1983, which involved a broader consideration of different privacy issues.[97]

The first report referred to the way that computerisation had changed the way that information of the sort included in the census (such as religion, marital status and income) was collected. It noted that computers had led to 'a radical increase in the capacity of record systems to store and retrieve personal information' with its associated cost savings.[98] Although the Law Reform Commission found that public concerns around these issues were valid, it did not recommend any major changes at that stage, given the broader consideration of different privacy issues being undertaken at the time as part of *ALRC Report 22*.[99]

The second Law Reform Commission report stated that privacy was in danger, identifying the chief sources of danger as growing official powers, new business practices and new information technology.[100] It referred to the issues raised by the 'extensive and expanding use of computers to process personal information in public and private administration' including the vulnerability of information-handling networks.[101] The Commission recommended that a Privacy Act be passed to establish information privacy principles and to provide for the appointment of a Privacy Commissioner. It also recommended that the Australian privacy regime should be consistent with privacy protections implemented in other jurisdictions on

---

95 See the Morison Report 1973 (Report on the Law of Privacy to the Standing Committee of Commonwealth and State Attorneys General No. 170/1973).

96 Law Reform Commission, *Report 12: Privacy and the Census* (1979) vi – vii ('*Privacy and the Census*').

97 Law Reform Commission, *Privacy (1976 - 1983), Report No 22* (1983) ('*Privacy (1976 – 1983)*').

98 *Privacy and the Census*, above n 95, 96.

99 Ibid

100 *Privacy (1976 – 1983)* above n 96, 4.

101 Ibid, 8.

the basis that, as part of an 'interdependent international community' it is important that solutions to common problems are compatible with 'those developed in countries with which Australia is inextricably involved, and with which it shares common interests.'[102] In particular, it recommended the adoption of privacy principles based on the *OECD Privacy Guidelines*.[103] This recommendation was consistent with the views of the Honourable Michael Kirby,[104] the Chairman of the Law Reform Commission in Australia at the time, who had also chaired the OECD expert group responsible for the development and publication of the *OECD Privacy Guidelines*.[105] These highly influential guidelines were published in 1980, and have had a significant impact on the development of member privacy legislation throughout the world, including Australia.[106]

## 2.2 THE AUSTRALIAN *PRIVACY ACT*

The Australian *Privacy Act*, adopting the model put forward in the *OECD Privacy Guidelines* and otherwise implementing many of the ALRC recommendations, was passed in 1988. The Act was significantly amended in 2000 when it was extended to apply to private entities.[107] It was amended again in December 2012,[108] which amendments became effective in March 2014. As

---

102 Ibid.

103 *Privacy (1976 - 1983)*, above n 96, 8.

104 About Michael Kirby (October 2014) <http://www.michaelkirby.com.au/index.php?option=com_content&view=article&id=67&Itemid=2>

105 Justice Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy' (2011) 1(1) *International Data Privacy Law* 6

106 See Graham Greenleaf, 'The Influence of European Data Privacy Standards outside Europe: Implications for globalization of Convention 108' (2012) 2(2) *International Data Privacy Law* 68; and Graham Greenleaf, 'Global Data Privacy Laws: 89 Countries, and Accelerating' (2012) 112 *Privacy Laws & Business International Report, Issue* 11-175; Justice Michael Kirby, 'The history, achievement and future of the 1980 OECD guidelines on privacy' (2011) 1(1) *International Data Privacy Law Journal* 6.

107 *Privacy Amendment (Private Sector) Act 2000* (Cth).

108 Ibid.

discussed, this research will focus on those provisions of the Act that were in effect prior to March 2014.[109]

The Act listed a set of Information Privacy Principles (IPPs)[110] that were the base line privacy standards applying to all Australian and ACT government agencies. Following the amendments in the year 2000, the Act also included a separate set of National Privacy Principles (NPPs)[111] that applied to those private sector organisations covered by the Act. Ten NPPs covered the collection, use and disclosure and secure management of personal information.

The Act specifically provides that organisations covered by the Act shall not breach a privacy principle.[112] In addition to the Commonwealth *Privacy Act*, a number of State Acts cover the protection of personal and health information by State government agencies.[113] These largely follow the same form as the Commonwealth *Privacy Act*. As discussed in Chapter 1.4, this thesis will examine the application of NPP 4 as part of the Commonwealth *Privacy Act*.

## 2.3 NPP 4

National Privacy Principle 4 was written in two parts. National Privacy Principle 4.1 (NPP 4.1) reflected the wording of the security principle in the *OECD Privacy Guidelines* and required those organisations it applied to, to 'take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification or disclosure.'[114] The purpose of NPP 4.1 was not only to prevent unauthorised access, modification or disclosure of personal information (whether directly by an organisational employee or indirectly as the result of a malicious third party such as a hacker) but also to protect against other

---

109 See Chapter 1.4.

110 *Privacy Act* Schedule 2. The IPPs have now been replaced.

111 Ibid Schedule 3. The NPPs have now been replaced.

112 *Privacy Act* s 16.

113 See Appendix D for a list of Australian State Privacy legislation.

114 *Privacy Act* Schedule 3 National Privacy Principle 4.1

categories of risk covered by the terms 'misuse' and 'loss.' These terms include, for example, unauthorised use by authorised personnel and the corruption of data.[115]

The second limb, National Privacy Principle 4.2 (NPP 4.2), had a much narrower operation. It required an organisation 'to take reasonable steps to destroy or permanently de-identify personal information if it was no longer needed for any purpose for which the information may be used or disclosed under National Privacy Principle 2.'[116] Information security theorists regard secure disposal as a sub-part of information security management, and a specific area for the implementation of controls.[117] This research will focus on the more general requirement to take 'reasonable steps' in NPP 4.1, recognising that a failure to take reasonable steps to securely dispose of data may be both a breach of the general requirement in NPP 4.1 and the more specific requirement in NPP 4.2.

NPP 4 was considered by the ALRC as part of its 2008 review of the *Privacy Act*. The questions posed in relation to NPP 4 by the review included:

- Is the scope of NPP 4 relating to the obligations of an organisation to secure data adequate and appropriate; and
- Should the IPPs and the NPPs regulate the deletion of personal information by organisations and agencies?[118]

The ALRC concluded that no significant change was required to NPP 4 other than the unification of NPP 4 and IPP 4 together into a single 'Australian Privacy Principle.'[119] A similar unification was also recommended for the other NPPs and

---

115 Waters, Greenleaf and Roth, above n 57. 6.

116 *Privacy Act* Schedule 3 National Privacy Principle 4.2.

117 See, eg, *ISO 27002*, above n 49, Section 11.2.7 which refers to the secure disposal and re-use of media as one of the 114 different controls that might be selected to mitigate information security risks.

118 *For your information*, above n 32, [4-17] –[4-19].

119 *For your information,* above n 32, Chapter 28.

IPPs.[120] Accordingly, the *Privacy Amendment Act*[121] introduced a new APP11 titled 'Security of Personal Information,' which replaced NPP 4 and IPP 4 but which is substantively the same as the previous two principles. The word 'interference' has been added to 'protection from unauthorised access, modification or disclosure' to make it clear that the protection must extend to computer attacks and other attacks that might not be covered by the other terms.[122] The reference to 'reasonable steps' has been changed to 'take such steps as are reasonable in the circumstances.'[123] The Explanatory Memorandum notes that this change is to make it clear that the assessment is an objective one 'but when considering what are objectively reasonable steps, the specific circumstances of each case must be considered.'[124] It is not expected that the amendment will have any major substantive effect.[125]

This research will focus on NPP 4, rather than APP 11, although some consideration of the operation of the new principle is included in the final chapter.

As previously discussed, all of the main international instruments on data protection include a requirement that organisations must take 'reasonable care' to secure personal information.[126]

The *OECD Privacy Guidelines* provide that '[p]ersonal data should be protected by reasonable security safeguards,'[127] which is the most broadly expressed version of the principle. NPP 4 adopts this broad wording from the *OECD Privacy*

---

120 *For your information,* above n 32, Executive Summary 'The *Privacy Act* and Privacy Principles.'

121 *Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth).

122 Explanatory Memorandum, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012' 86 ('*Explanatory Memorandum'*).

123 The wording of APP 11 is different to that proposed by the ALRC for the data security principle. See *For your information,* above n 32, [28.105].

124 *Explanatory Memorandum*, above n 122, 54.

125 Alexander, Koster and Paterson, above n 67.

126 See discussion in Chapter 1.5.2.

127 The Security Safeguards Principle 11, Part 2 of the *OECD Privacy Guidelines* provides: 'Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.' *OECD Privacy Guidelines*, above n 24.

*Guidelines*. Article 17 of the *EU Data Protection Directive* requires organisations to protect personal data by implementing 'appropriate technical and organisational measures.'[128] In determining what measures may be appropriate, the provision refers to ensuring 'a level of security appropriate to the risks represented by the processing and the nature of the data to be protected,' having regard to the state of the art and the cost of implementation of the measures. [129]

The security principle in the APEC Privacy Framework is also more comprehensive than the OECD provision. It refers to the implementation of safeguards which should be:

> proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review and reassessment.[130]

The APEC Framework also refers to risk, the relationship between the measure to be implemented and the 'likelihood and severity' of harm and the need for those safeguards to be subject to regular review. Risk, the use of risk to select 'proportional' security measures and the need for periodic review, are all part of the industry practice approach to security considered further in the next chapter.

## 2.4 OVERVIEW OF THE OAIC'S FUNCTIONS AND POWERS

The role of Privacy Commissioner was created by the *Privacy Act* in 1988. The Privacy Commissioner was originally supported by the Office of the Privacy Commissioner (OPC). In 2010, the OPC became part of the Office of the Australian Information Commissioner (OAIC), which is headed by the Australian Information Commissioner (AIC), which office also includes the Office of the Freedom of Information Commissioner.[131] The Privacy Commissioner currently reports to the

---

128 EU Data Protection Directive 95/46, above n 25, Article 17.1.

129 Ibid.

130 APEC Privacy Framework, above n 26, Principle 22

131 *Australian Information Commissioner Act 2010* (Cth).

AIC, but maintains the same functions and powers, albeit with some new constraints.[132] It has been proposed that the OAIC will be disbanded and the Privacy Commissioner's functions will be undertaken by the Commissioner acting in an independent statutory position within the Human Rights Commission, however these changes seem to be on hold.[133] The implications of this change are considered briefly at the end of this research.

The Commissioner has a broad range of functions. Prior to March 2014 they included:

- Monitoring and research;[134]
- Advice;[135]
- Education;[136] and
- Guidance, including publishing binding guidelines and non-binding fact sheets, information sheets and guidelines.[137]

---

132 Ibid s 12. See also Carolyn Adams, 'One office, three champions? Structural integration in the office of the Australian Information Commissioner' (2014) 21 *AJ Admin L* 77.

133 John McMillan, Australian Information Commissioner, James Popple (Freedom of Information Commissioner) and Timothy Pilgrim, Privacy Commissioner, 'Australian Government's Budget decision to disband OAIC' (Statement, 13 May 2014) < http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/australian-government-s-budget-decision-to-disband-oaic>. The re-structuring is proposed in the Freedom of Information Amendment (New Arrangements) Bill (Cth) which was introduced into the Senate but not considered before the end of the 2014 sitting period. The current status of that Bill is available at Parliament of Australia, Freedom of Information Amendment (New Arrangements) Bill 2014 (Cth) <http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r5350>. The OAIC has advised that it will 'remain operational until further notice.' Office of the Australian Information Commission, *OAIC to remain operational until further notice* (December 2014) <http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/oaic-to-remain-operational>.

134 *Privacy Act* s 27(1)(b).

135 Ibid s 27(1)(j).

136 Ibid s 27(1)(m).

137 Ibid s 27 (1)(e), 'to prepare and publish in such manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices ... that may ... be interferences with the privacy of individuals ...'. This is in addition to the power to issue guidelines relating to approved privacy codes, and under the *Data Matching Program (Assistance and Tax) Act 1990* (Cth) and s 135AA of the *National Health Act 1953* (Cth).

These functions, together with the power to audit public entities,[138] were grouped together and referred to as 'oversight' functions by the ALRC.[139]

The individual appointed as Commissioner is given the power to do all things necessary or convenient to be done for or in connection with the performance of these functions.[140]

In addition to these oversight functions, the Commissioner also has an investigation and enforcement role. The Commissioner can investigate complaints and can also conduct investigations on its own motion.[141] The Commissioner can make a determination following complaint-based investigations, which may include the award of compensation and requiring the rectification of practices.[142] In this research, given the low number of determinations made to date,[143] these enforcement powers will be referred to as the 'investigation' powers of the Commissioner.

The Commissioner's oversight and investigation powers have been extended by the recent amendments to the *Privacy Act*. The Commissioner's new powers include the ability to:

- Conduct an assessment of the maintenance of personal information of a private organisation (referred to as the privacy assessment power). This is similar to the pre-existing power to audit public entities;[144]

---

138 *For your information,* above n 32, [47.87] - [47.116].

139 Ibid [47.2]-[47.22].

140 Pursuant to the *Privacy Amendment Act*, a new s 27(2) will be inserted which will confirm that the Commissioner has the power to do all things necessary or convenient to be done in connection with the performance of those functions *Privacy Act*.

141 *Privacy Act* ss 36, 40.

142 Ibid s 52.

143 The Commissioner's use of the power to make a Determination which was the major enforcement power available prior to March 2014, other than carrying out investigations, is discussed further in Chapter 7.3.

144 *Privacy Act* s 33C.

- Accept written, enforceable undertakings by entities[145] and, if an undertaking is breached, apply to the Federal Court for an order directing the entity to comply with the undertaking or any other order the court considers appropriate; [146]
- Make a determination after an own motion investigation;[147]
- Include in a determination any order that it considers necessary or appropriate;[148] and
- Apply to court for the imposition of civil penalties for a serious or repeated interference with the privacy of an individual. [149]

As these new functions only became effective in March 2014, there has been little opportunity to determine how they will be used by the Commissioner, particularly in regard to NPP 4. Therefore reference is included for the sake of completeness only, although reference to the effect that some of these powers may have in terms of the findings of this research is included in the final Chapter.

Taken together, the Commissioner can provide policy advice to government and parliamentary inquiries, issue binding and non-binding guidelines, provide education and receive, investigate, and determine the outcome of complaints. The OAIC has acknowledged the breadth of its different function and powers, noting that: 'Taken together, these functions cast the OAIC in the roles of regulator, decision maker, adviser, researcher and educator.'[150] The uniqueness of investing a government-created role with this broad mix of powers and functions, which fall

---

145 Ibid s 33E.

146 Ibid s 33F.

147 Ibid s 52(1A).

148 Ibid s 52(3A).

149 Ibid. Pt VIB deals specifically with civil penalty orders.

150 Alan Hawke, 'Review of the Freedom of Information Act 1982 and Australian Information Commissioner Act 2010' (Australian Government, 2014) <http://www.ag.gov.au/Consultations/Pages/ReviewofFOIlaws.aspx>. See also *OAIC 2012 Annual Report*, above n 1, 4.

across all parts of the 'legislative', 'executive' and 'judicial' spectrum, has been remarked upon.[151]

To understand why the Privacy Commissioner has been given such a broad range of powers, including both oversight and investigation powers, and how it is anticipated that these powers will be exercised, it is important to understand the regulatory foundations underpinning the *Privacy Act*. An appreciation of these foundations and the related assumptions about the regulatory interactions required to support their successful implementation will help inform this analysis of the Commissioner's use of its powers to support compliance with NPP 4.

## 2.5 REGULATORY FOUNDATIONS

The *Privacy Act* is based on the twin foundations of principle-based regulation and a compliance approach to enforcement.[152]

### 2.5.1 Principle-Based Regulation

In introducing a privacy regime based on the *OECD Privacy Guidelines*, the Australian Government accepted a principle-based regulatory model for the protection of personal information in Australia.[153] Principle-based regulation (PBR) was confirmed as the appropriate regulatory model for privacy on the introduction of the private sector provisions in 2000[154] and as part of the OPC review in 2005.[155] PBR was confirmed again by the ALRC in 2008, after the ALRC gave specific consideration to the issue.[156]

---

151 Philip Schutz, 'Accountability and Independence of Data Protection Authorities - A Trade Off?' in Daniel Guagnin et al (eds), *Managing Privacy through Accountability* (Palgrave Macmillan, 2012); Kevin O'Connor, above n 65, 233.

152 *For your information,* above n 32, Chapter 4.

153 Ibid [2.4], [18.24].

154 Commonwealth, *Parliamentary Debates*, House of Representatives, 8 November 2000, 22370 (D Williams, Attorney-General).

155 Office of the Privacy Commissioner, 'Getting in on the Act: The Review of the Private Sector Provisions of the *Privacy Act* 1988' (2005) ('*Getting in on the Act*').

156 *For your information,* above n 32, Chapter 4.

Principles can be distinguished from bright line rules (as defined below) and complex or detailed rules, examples of which are included in the table below.[157]

| Bright line rule | Principle | Complex/detailed rule |
|---|---|---|
| An organisation must not collect personal information relating to an individual's sexuality | An organisation must not collect personal information unless it is necessary for one of its functions or activities | An organisation [defined] must not collect [defined] personal information [defined] unless all of the following conditions are met: [list of conditions]. |

*Table 1: Examples of different types of regulatory provisions*[158]

A 'bright line' rule contains a single criterion of applicability. Their simplicity means bright line rules are straightforward and so easier to understand and apply than principles; however, they are susceptible to gaming and 'creative' compliance. The specificity of the rule means it may not be broad enough to capture all of the conduct that it is aimed at. Alternatively, an organisation may 'comply with the letter, but not the spirit, of the rule.'[159]

A complex or detailed rule can provide a higher degree of certainty by providing greater detail about what is required for compliance. However, the greater degree of specificity means that these rules are even more susceptible to manipulation and creative compliance than bright line rules.[160]

In comparison, a 'principle' articulates substantive objectives rather than specific compliance requirements.[161] The perceived benefits of principle-based regulation include being less susceptible to gaming and a 'tick box' compliance

---

157 J Black, *Principles Based Regulation: Risks, Challenges and Opportunities* (London School of Economics and Political Science, 2007) 10.

158 *For your information,* above n 32, Table 18.1.

159 Ibid [18.28].

160 Ibid [18.30].

161 Ibid [18.29].

approach. Principles give firms 'increased flexibility to decide more often … what business processes and controls they should operate.'[162] It is believed that the devolution to the regulated community of the interpretation of compliance obligations will result in an industry that deals with regulatory issues in a more effective and efficient way. Principles are also seen as more flexible than prescriptive rules and therefore more durable in a rapidly changing environment.[163] It is this durability aspect that was stressed by the ALRC in its review of the appropriateness of the principle-based regulatory scheme, particularly when considering the challenges posed by new technology.[164] While concluding that the advantages of PBR outweighed the drawbacks, the ALRC identified that one of the issues with principles was certainty as to what was required for compliance:

> While principles may appear simple to apply — in that they are concise and avoid arcane language — problems can arise in practice where, for instance, there is a dispute as to the meaning of the key terms.[165]

The ALRC considered the level of detail and guidance that should be provided by the privacy principles themselves, noting that the choice of how prescriptive the principles should be reflected a wider policy choice about the degree to which the regulation of personal information should be 'light-touch.'[166]

Notwithstanding this commitment to PBR as the preferable regulatory model, the ALRC accepted that there were areas — health and research, credit reporting and telecommunications — where principles were 'not adequate to achieve the relevant policy objectives.'[167] For those areas, the ALRC recommended a 'hybrid' regulatory

---

162 Financial Services Authority U.K., *Principles Based Regulation: Focusing on the Outcomes that Matter* (2007) 6 – 7.

163 *For your information,* above n 32, [18.55].

164 Ibid, 235.

165 Ibid [18.29].

166 Ibid [18.35].

167 Ibid [4.37].

model (involving principles and rules), which it regarded as the best way to meet the competing needs of clarity, flexibility, simplicity and certainty.[168]

NPP 4 was not considered by the ALRC as a principle which should be supplemented by rules, unlike NPP 11, which covered use and disclosure.[169] However, the ALRC did consider that the Commissioner should issue separate non-binding guidance to support a clearer understanding of NPP 4.[170]

The ALRC drew particular attention generally to the importance of guidance from the regulator to support certainty as to the meaning of principles, stating that 'the principle-based regime cannot operate effectively unless there is such guidance.'[171] It also warned that care needed to be taken to ensure that guidance did not become de facto rules[172] or that confusion was caused by the proliferation of guidance.[173]

There is some suggestion that PBR equates to 'light-touch' regulation in the sense of it being more difficult to establish breach. The ALRC stated that the use of principles was an appropriate regulatory approach to business needs as a matter of policy because '[i]t is generally more difficult to establish a breach of high-level principles than provisions imposing detailed and specific obligations.'[174] This was subsequently clarified when the ALRC confirmed the 'long-standing policy position' that the *Privacy Act* should be light touch 'in the sense that it should provide only such regulation as is required to protect individuals' privacy without unreasonably burdening the public or private sectors.'[175]

---

168 Ibid [4.37], [18.57] - [18.59].

169 Ibid [4-34].

170 Ibid Recommendation 28-3.

171 Ibid [4-59]. The use by the Privacy Commissioner of its guidance powers is discussed further in Chapter 6.

172 Ibid.

173 Australian Law Reform Commission, *Reviewing the Privacy Act,* Issues Paper No 31 (2006).

174 *For your information,* above n 32, [18.35].

175 Ibid [18.62].

In its guide to regulation, the Australian Government referred to PBR generally as a type of 'light touch regulation', noting the benefits it provides through allowing maximum flexibility among the regulated community regarding how they achieve compliance.[176] It also noted that PBR must be implemented properly to ensure that those affected understand their legal rights and obligations, otherwise the regulation may not be effective.[177] However, little further elucidation on what that proper implementation might entail is provided in the guide.

The role of the regulator and the methods they use to engage with the regulated community to ensure compliance are important to PBR. One of the assumptions supporting principle-based regulatory theory is that the market is self-correcting and that responsible organisational management will ensure the adoption of appropriate systems and processes to meet the outcomes stated in the principles.[178] However, to ensure that the market operates in the expected way, there must be:

- Close engagement between the regulator and the regulated based on mutual trust;
- Outcomes and goals clearly communicated by the regulator; and
- A predictable enforcement regime.[179]

In her more recent work, Black underlined the importance of close engagement between the regulator and the regulated community, referring to the need for a dense

---

176 Australian Government, 'The Australian Government Guide to Regulation' (2014) <http://www.cuttingredtape.gov.au/sites/default/files/documents/australian_government_guide_regulation.pdf>, 28. See also *For your information,* above n 32, [18.35]. The idea that good regulation is light handed is not necessarily shared by the academic literature which agures the opposite, that light handed regulation 'requires significantly greater levels of attention to risk reduction than that required under previous 'command and control' regimes.' Fiona T Haines and Nick Taylor, *The Paradox of Regulation: What Regulation Can Achieve and What it Cannot* (Edward Elgar, 2011) 8.

177 Ibid.

178 Baldwin, Cave and Lodge, *The Oxford Handbook of Regulation* (Oxford University Press, 2010) 302 – 303.

179 Julia Black, 'Forms and paradoxes of principles-based regulation' (2008) 3(4) *Capital Markets Law Journal* 425.

network of 'regulatory conversations' between the regulator and the regulated regarding the purpose and application of the principle, where the outcome is structured around the goal that the principle is trying to achieve. [180] Black noted that principles give the regulated more discretion in what they do, so that responsibility for ensuring that the objectives of the principles are met is shifted in part from the regulator to the regulated.[181] According to Black, this involves 'a significant shift in responsibility to firms and requires a substantially different set of skills on the part of inspectors and compliance staff to engage in the negotiations and qualitative judgement that are entailed.'[182] The shift in responsibility also involves a conscious and deliberate focus by the regulator on the firm's internal systems of management and controls.[183]

Finally, Black referred to the importance of regulators managing the greater interpretive risk for firms that arise from the use of principles, and minimising the effects of this risk through its enforcement approach.[184] Black's view was that if a regulator were to take a punitive approach to every minor infraction it would lead to a demand for rules. Enforcement therefore 'has to be responsive to the firm's own attitude and behaviour' and focus on outcomes.[185]

In other words, PBR requires a closely engaged regulator using a responsive enforcement approach to achieve clearly communicated outcomes and goals as part of a two-way conversation, while focusing on the operation of organisational management systems and controls.

---

180 Julia Black, 'The Rise, Fall and Fate of Principles Based Regulation' (Working Paper no 17, London School of Economics and Political Science, 2010) 6.

181 Ibid 7.

182 Ibid 8.

183 Ibid.

184 Ibid 6 -7.

185 Ibid 7-8.

### 2.5.2 Compliance Approach

The *Privacy Act* is based on a particular type of approach to compliance referred to as responsive regulation.[186] This is consistent with Black's view of the importance of a responsive regulatory approach in a principle-based system.[187]

Responsive regulation takes account of the relationship between regulation and those being regulated, and offers a graduated approach to enforcement.[188] A responsive approach to regulation was first articulated by Ian Ayres and John Braithwaite.[189] It provided an alternative to traditional 'command and control' enforcement approaches and a potential middle ground between the public interest in regulating businesses and the interest of businesses in reducing state intervention.[190] Responsive regulation is based on the contention that, in order to be effective, efficient and legitimate, regulatory policy should take neither a solely deterrent nor a solely cooperative approach. It proposes a regulatory pyramid with different regulatory actions to be taken when responding to the non-compliance of different types of organisations. [191]

The pyramid arranges enforcement strategies in a hierarchy with more cooperative strategies deployed at the base of the pyramid and progressively more punitive approaches utilised only if, and when, cooperative strategies fail. The pyramid recognises the three types of regulatees. First, at the base of the pyramid, and forming the biggest group, is the organisation or individual who is presumed to be willing to comply but who may be misinformed or lacks knowledge about their compliance obligations. Second, in the centre of the pyramid, is the organisation or

---

186 *For your information*, above n 32, Chapter 4.

187 Black, above n 180 and Black, above n 179, 440 – 441.

188 Vibeke Lehmann Nielsen and Christine Parker, 'Testing Responsive Regulation in Regulatory Enforcement' (2009) 3(4) *Regulation and Governance* , 4.

189 I Ayres and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992).

190 C. Sunstein and R. Thaler, *Nudge* (New Haven, 2008) 2.

191 Ayres and Braithwaite, above n 189, Chapter 2. Also referred to in *For your information,* above n 32, [47.19]

individual who needs incentives to comply. Third, at the top of the pyramid is the irrational organisation or individual or the knowing offender whose actions require a much heavier sanction.

The pyramid model emphasises that most effort should be directed towards initiatives at the base of the pyramid, which will address the most common reasons for non-compliance. Escalation to responses higher in the pyramid should occur only when efforts to secure compliance through guidance and education have failed.

Regulatees who demonstrate a willingness and ability to correct any harm they have caused and to become compliant should be treated less harshly than those who fail to cooperate in response.[192] The regulator should go on to 'somewhat punitive' action 'only reluctantly and only when dialogue fails, and then escalate to even more punitive approaches only when the more modest forms of punishment fail.'[193] When they become willing to cooperate, the regulator should, according to Ayres and Braithwaite, be able to forgive a history of wrongdoing and de-escalate down the pyramid to less harsh enforcement.[194]

To ensure the effective administration of the responsive regulatory system in question, it is also important to have a specific regulator in place.[195] One of the main roles of the regulator is to provide education and guidance regarding what is required to be compliant, particularly where the legislative framework is principle-based. When used with a PBR in particular, compliance is dependent on a shared understanding of what the principles mean and how they are to be applied. This understanding is developed through iterative and reflexive communications between regulator, regulatee and others as to the purpose and application of the principle.[196]

---

192 Ibid 19; J Braithwaite *Restorative Justice and Responsive Regulation* (Oxford University Press, 2002) 31.

193 Braithwaite, above n 192.

194 Ayres and Braithwaite, above n 189, 33.

195 Ibid 69.

196 Black, above n 179, 439.

In its review of the regulatory underpinnings of the *Privacy Act*, the ALRC supported responsive regulation. It noted its focus on achieving outcomes, calling it a 'useful framework to administer a principles-based regime such as the *Privacy Act.*'[197] The Ayres and Braithwaite enforcement pyramid and their contention that compliance is 'most likely' when a regulator displays an explicit enforcement pyramid were referred to with approval.[198]

Outside the work of the ALRC, the use of a responsive approach to ensure compliance with the *Privacy Act* has been generally supported, [199] although there has also been some criticism about the particular way that Commissioners have elected to use the range of available functions and powers in pursuance of a responsive approach.[200] The Privacy Commissioner has expressly referred to the enforcement pyramid as central to the OAIC's approach to enforcement activity,[201] also describing its enforcement approach as 'an escalation model that includes a range of regulatory responses.'[202]

---

197 *For your information,* above n 32, [4.25].

198 Ibid.

199 Allan Fels, 'The Role of The Privacy Regulator in an Era of Transparency' (Paper presented at the 25th International Conference of Data Protection and Privacy Commissioners, September 2003); Bendall, above n 65, O'Connor, above n 65; Hummerston, above n 65; Alexander, Koster and Paterson, above n 65.

200 See, eg, Graham Greenleaf, Nigel Waters and Lee A Bygrave, above n 65; Graham Greenleaf, Nigel Waters and Lee Bygrave, '*Implementing Privacy Principles: After 20 Years, It's Time to Enforce the Privacy Act*' [2007] *UNSWLRS* 31; *Weaker Principles*, above n 65, 16; *Making Privacy Law Safe*, above n 65.

201 Timothy Pilgrim, Privacy Commissioner, 'Privacy Reform – Act Three' (Presentation to the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013).

202 John McMillan, Australian Information Commissioner, and Timothy Pilgrim, Privacy Commissioner, 'The OAIC's enforcement approach to new privacy laws from 12 March 2014' (Statement from the Australian Information Commissioner and Privacy Commissioner, 28 February 2014), < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/oaic-enforcement-approach-to-new-privacy-laws-12-march-2014/the-oaic-s-enforcement-approach-to-new-privacy-laws-from-12-march-2014-statement-from-the-aust>.

## 2.6 EXERCISE OF REGULATORY POWERS

The responsive use of a broad range of powers means in practical terms that the regulator has many different options for the use of powers to secure compliance.

In 2001, the Commissioner provided guidance on the way it intends to use its powers to promote compliance with the *Privacy Act*.[203] Issued following the extension of the Act to private entities, the guide's underlying premise is that the Commissioner will seek to strike a balance between ensuring privacy protection and not unduly burdening relevant organisations.[204] The guide explicitly reflects a responsive regulatory approach, stating that the OPC's 'first and preferred approach at all times' will be to provide advice, assistance and information, rather than punishment.[205] In summary, the guide:

- Outlines the process for investigating and resolving complaints;[206]
- Refers to own motion investigations, providing that the OPC will take the same approach to OMIs as it does to complaint-based investigations;[207]and
- Outlines how the Commissioner will publicly report on its use of powers.[208]

In terms of the underlying principles guiding the exercise of powers, the guide makes only two statements. The first is that the OPC will act in a way which is open and predictable. In particular, it will 'not take action in relation to an organisation without first giving it fair warning.'[209] The second is that the action taken by the OPC will be proportional to its seriousness. Factors relevant to the assessment of the seriousness of any matter include the number of people affected and the disadvantage

---

203 Office of the Privacy Commissioner, '*Private Sector Information Sheet 13 - The Privacy Commissioner's Approach To Promoting Compliance With The Privacy Act*' (2001) ('*Information Sheet 13*').

204 Ibid 1.

205 Ibid 2.

206 Ibid.

207 Ibid 3.

208 Ibid.

209 Ibid.

they may suffer together with the 'willingness of the organisation to take action to resolve the matter and to prevent recurrence.'[210] This last aspect is again consistent with a responsive regulatory approach.

The ALRC referred to the regulated community's understanding of the basis on which the OAIC will use its powers as fundamental to the success of the responsive regulatory approach.[211] To assist in the community's understanding, the ALRC suggested that the Commissioner publish a clear policy on the use of its powers. The ALRC believed that such a policy would act as an incentive for compliance and would also allow the regulator to discriminate between organisations that were genuinely trying to comply and those that were not.[212]

In terms of the exercise of its powers, the ALRC was of the view that if the Commissioner was both using, and seen to be using, a wide range of strategies to ensure compliance with the *Privacy Act*, the 'benefits of specific and general deterrence that can be generated by a transparent, balanced and vigorous enforcement approach can be achieved.'[213] The ALRC did not take the opportunity to comment on the 2001 guide.

The ALRC's position that the Commissioner's powers should be exercised in a way which is transparent, balanced and vigorous is broadly consistent with the commitment to the open, predictable and proportional exercise of powers expressed in the 2001 guide.

The proposition that the Commissioner's use of its powers should be transparent, balanced and vigorous is also consistent with the other models for regulatory action. For example, Malcolm Crompton, the Australian Privacy

---

210 Ibid.

211 'A clear enforcement policy that outlines what the OPC's usual response to a particular type of breach will be … can provide incentives for agencies and organisation to put in place … mitigating practices.' *For your information,* above n 32,[45.26].

212 Ibid.

213 Ibid [4.73] - [47.4].

Commissioner from 1999–2004,[214] proposed a framework for assessing the performance of privacy regulators. According to this framework, a privacy regulator would be assessed based on transparency, among other things, in regard to its enforcement and complaint-handling roles.[215] Other criteria suggested by Crompton included independence, fairness and accountability, which arguably are part of transparency when applied to investigations and reporting. These elements are discussed in more detail in the next section, which considers procedural fairness as part of transparency.

The United Kingdom Information Commissioner's Office (ICO) has issued a *Data Protection Regulatory Action Policy*[216] that outlines the ICO's strategy for ensuring compliance. According to this policy, the UK ICO's powers will be used where personal information is at risk because obligations are deliberately or persistently ignored, examples need to be set, or the interpretation of the law is in doubt.[217] This policy further provides that regulatory action taken by the ICO will be consistent with the five principles of good regulation that UK regulatory bodies must have regard to: transparency, accountability, proportionality, consistency and targeted responses.[218] The UK ICO policy expands on the idea of transparency. It provides that the ICO will be open regarding the regulatory action taken, making information about the cases pursued, their nature and the outcomes available on its

---

214 Malcolm Crompton, 'Are Comparisons Possible? A framework for assessing the performance of data protection supervisors' (Paper presented at 27th International Conference of Data Protection and Privacy Commissioners, Montreux, Switzerland, 15 September 2005) <http://www.iispartners.com/Publications/index.html#reg>. See also Malcolm Crompton, 'Light Touch or Soft Touch?: Reflections of a regulatory implementing a new privacy regime' (Speech delivered at National Institute of Governance, University of Canberra, 18 March 2004); and Pat Barrett, 'Commentary on Malcolm Crompton's Paper entitled "Light Touch or Soft Touch?: Reflections of a regulatory implementing a new privacy regime"' (Speech delivered at National Institute of Governance, University of Canberra, 18 March 2004).

215 Ibid 6.

216 Information Commissioner's Office, *Data Protection Regulatory Action Policy Version 2.0* (UK Government, 2013) <http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-regulatory-action-policy.pdf>.

217 Ibid 1-2.

218 Ibid. These five principles for measuring and improving the quality of regulation and its enforcement were first set out by the UK Better Regulation Task Force. Better Regulation Task Force, *Principles of Good Regulation* (UK Cabinet Office, 2003).

website and in its annual reports. [219] The policy also provides that, where regulatory action reveals problems that are common to a particular business sector or activity and it is apparent that there is a need for general advice on the issue in question, the ICO will make such advice available.[220]

Within the EU, the key statement on principles of good regulation is contained in the *Mandelkern Report*[221] which lists 7 'common principles' of regulatory quality which include proportionality, transparency and accountability.[222]

These guiding principles of transparency, accountability, proportionality and of consistency that are used by various governments to assess regulatory actions are consistent with the ALRC's principles of transparency, balance and vigour. The concept of proportional use of powers is synonymous with the idea of a balanced yet vigorous response akin to the regulatory principles inherent in PBR and responsive regulation. Similarly, the idea of consistency can also be included within an assessment of whether the response has been balanced.

'Accountability' is a little more complex. It falls within the idea of transparency, at least to the extent that the Commissioner should be able to be held accountable for the way in which its powers have been used. Transparency as an accountability mechanism introduces considerations of procedural fairness and reasons for decisions, which is discussed in more detail in the following section. The more general question as to whether the Commissioner has acted appropriately so as to be held accountable having regard to the review and appeal provisions provided within the *Privacy Act* is outside the scope of this research.[223]

---

219 Information Commissioner's Office, above n 215.

220 Ibid.

221 Mandelkern Group on Better Regulation *Report on Better Regulation, Final Report* (European Commission, 13 November 2001) <http://ec.europa.eu/smart-regulation/better_regulation/documents/mandelkern_report.pdf>.

222 R Baldwin, *Better Regulation: Is it better for business?* (Federation of Small Business, 2007).

223 For consideration of the accountability of the Privacy Commissioner, see the references above n 65.

It is proposed that the criteria put forward by the ALRC, that the exercise of regulatory powers should be transparent, balanced and vigorous will be used as part of the conceptual framework used to assist in answering the third research question of this research: To what extent is the exercise of the Commissioner's powers consistent with principles for the exercise of regulatory powers?

The framework will be applied to the consideration of the use of both the Commissioner's oversight powers and to the use of the investigation powers. It will include, for example, consideration of the following:

| | |
|---|---|
| Transparency | • Openness about the use of powers, including the reasons for the use of powers;<br>• Openness about the outcomes achieved; and<br>• Assistance in understanding how the Commissioner interprets the law. |
| Balance | • Consistency of the use of powers;<br>• Proportionality of use of powers; and<br>• Whether powers have been used in a targeted manner to address areas of greatest risk. |
| Vigour | • Frequency of the use of powers;<br>• Types of powers which have been used; and<br>• Timeliness of the use of powers. |

As already referred to, there are additional facets to the idea of transparency which are raised in the context of the use of the Commissioner's investigation powers. In 2003, Professor Greenleaf considered how to assess the Commissioner's

reporting on the use of its investigation powers.[224] Two criteria were proposed for that assessment: first, whether the reports help interested parties understand how the Commissioner interprets the privacy law(s) of the jurisdiction; and second, whether they help all relevant parties understand the range of outcomes reached in individual complaints and whether those outcomes provide reasonable redress for the complainants, while only imposing reasonable burdens on the respondents.[225] These criteria are consistent with ideas of transparency, particularly in regard to decision-making, and balance. However, in the context of the use of the investigation powers, they also raise questions of procedural fairness, in particular whether the investigation provided the complainant with reasonable redress. When considering the use of the investigation powers (as opposed to the oversight powers) and particularly the decisions made based on those investigations and the reporting of those decisions, additional considerations could be regarded as part of the transparent, balanced and vigorous use of such powers. [226] These considerations are covered by the broad concept that, when carrying out investigations and making and reporting on decisions, a regulator should act in accordance with the principles of procedural fairness.

### 2.6.1 Procedural Fairness and the Investigation Powers

The OAIC has acknowledged that it will use its investigation powers in accordance with the principles of procedural fairness.[227] Administrative law texts

---

224 *Reforming reporting of privacy cases*, above n 65.

225 Ibid.

226 See, eg, Michael Head, *Administrative Law Context and Critique* (The Federation Press, 3rd ed, 2012) 186; and Sarah Withnall and Michelle Evans, *Administrative Law* (LexisNexis Butterworths, 2010) Chapter 11.

227 Office of the Australian Information Commissioner, 'Privacy Complaints and Procedures Manual' <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/privacy-complaints-practice-and-procedure-manual/file-management-and-security-standards> (‘*Complaints Manual’*), 14; which includes a section headed ‘Good Decision Making and Procedural Fairness’. This document is no longer published on the OAIC’s website. A copy is available from the researcher. The OAIC’s commitment to the principles of both procedural fairness and good decision making was confirmed in the draft policy issued in March 2014, Office of the Australian Information Commissioner, ‘Privacy Regulatory Action Policy

identify three common law rules implicit in procedural fairness.[228] The three elements or rules on which procedural fairness are based are:

- The right to a fair hearing;
- The bias rule; and
- The evidence rule.

Compliance with these same three rules is recognised by the Commissioner as part of the framework for its use of its investigation powers in its *Complaints Manual*.[229]

#### 2.6.1.1 The right to a fair hearing rule

The fair hearing rule requires that a person must be allowed an adequate opportunity to present their case where certain interests and rights may be adversely affected by a decision-maker. In the OAIC's context this is interpreted as requiring that the respondent be advised of the allegations in as much detail as possible, be advised of possible outcomes, be given the opportunity to reply to the allegations and, where appropriate, allowed an opportunity to comment on any proposed finding before the final decision is made.[230]

In assessing the use by the Commissioner of its investigation powers, this research will consider the extent to which each respondent was:

- Advised of the allegations;
- Advised of the possible outcomes;
- Given an opportunity to reply to the allegations; and
- Allowed to comment on proposed findings before the final decision.

---

(draft)'(March 2014) <http://www.oaic.gov.au/news/consultations.html#info_security> ('*Regulatory Powers Policy*').

228 See, eg, Head, above n 225, 186; and Withnall and Evans, above n 225, Chapter 11.

229 *Complaints Manual* above n 227, 14.

230 Ibid.

#### 2.6.1.2 The bias rule

The second rule, the bias rule, states that no one ought to be judge in his or her own case.[231] This requires that the deciding authority be unbiased during the hearing or making the decision. Consideration of this issue is outside the scope of this research.

#### 2.6.1.3 The evidence rule

The third rule is that any findings must be based upon logically probative material.[232] This is reflected in the *Complaints Manual*, which provides that case officers and decision-makers should be able to clearly point to the evidence on which findings are based.[233] The standard of proof is the civil standard: the balance of probabilities, that is, that based on the evidence it is more probable than not that the alleged breach occurred.[234]

The *Complaints Manual* does not provide detailed guidance about the method for identifying or collecting relevant evidence or how a decision is to be made by reference to that evidence. It does confirm that, to ensure procedural fairness, the 'OAIC needs to take account of all relevant considerations and needs to support its position with evidence or other material.'[235] The *Manual* refers to different types of evidence that might be available, including copies of audit trails from computer systems and 'corroborative evidence from third parties, often by way of a statutory declaration.'[236] The *Manual* suggests that further evidence-collecting steps might be considered, depending on the response to the initial request for information sent to the respondent entity. These steps might include requesting further information or

---

231 Ibid.

232 See Head, above n 226.

233 *Complaints Manual* above n 227, 14.

234 Ibid

235 Ibid.

236 Ibid 17.

documents from the respondent or complainant or seeking independent corroboration from another source, for example a website, government body or third party.[237]

In 2007, the Administrative Review Council (ARC) released a series of best practice guides designed for agencies with decision-making authority (which would include the Office of the Australian Information Commissioner). These include a guide on the role of decision-makers when receiving evidence, determining questions of fact and accounting for their findings, called the *ARC Evidence Guide*.[238] The *ARC Evidence Guide* distinguishes between material facts (facts required to be established by the regulator, for example, that the entity has taken reasonable steps to secure personal information) and relevant facts, which go towards establishing the material facts. According to the *ARC Evidence Guide*, '[t]he factual findings should form a chain of reasoning that leads logically from relevant facts through material facts to the decision.'[239]

The *ARC Evidence Guide* provides that a decision-maker such as the Privacy Commissioner must:

- Determine all material questions of fact;
- Not base a decision on a fact without evidence for that fact; and
- Ensure that every finding of fact is based on evidence that is relevant and logically supports the finding.[240]

Each of these criteria will be considered as part of the consideration of procedural fairness in the detailed review of the Commissioner's use of its investigation powers in Part 3 of this research.

The *Complaints Manual* does not distinguish between the evidence requirements in complaint-based investigations (where two parties provide evidence)

---

237 Ibid.

238 Administrative Review Council, *Decision Making: Evidence, Facts and Findings* (August 2007) <http://www.arc.ag.gov.au/Publications/Reports/Pages/Downloads/ARCBestPracticeGuide3EvidenceFactsandFindings.aspx> ('*ARC Evidence Guide*').

239 Ibid 2.

240 Ibid 1.

versus own motion investigations (which typically only involves a respondent). This possibly reflects the *Manual's* focus on complaint-based investigations. It might be expected that those cases where only the applicant or respondent provides evidence might be treated differently to more adversarial situations where opposing sides both put forward their own view of the facts. In own motion investigations (OMIs), it is likely that much of the information will be provided by the entity being investigated. The *ARC Evidence Guide* states that information provided by applicants (or respondents in the case of OMIs) may be used as evidence but only for 'establishing facts that are likely to be true or that are not material.'[241] This limitation is significant in OMIs and will be considered further in the analysis of the use of the investigation powers included in Part 3.

#### 2.6.1.4 Decision-making

The right to be given reasons for a decision is considered by some as another strand of procedural fairness and as part of good decision-making.[242] The Administrative Review Council supports providing reasons for a decision and regards it as an obligation that is part of the principles of good decision-making and procedural fairness.[243]

The provision by the Commissioner of reasons or adequate reasons for its decisions has been a contentious issue.[244] The *Privacy Act* does not require the Privacy Commissioner to provide any formal statement or reasons for a decision

---

241 Ibid 4.

242 See, eg, Head, above n 225, 186.

243 Administrative Review Council, *Decision Making: Reasons* (August 2007) < http://www.arc.ag.gov.au/Documents/Revised+Best+Practice+Guide+4+-+Reasons+-+24+April+2008.pdf > ('*ARC Decision Guide*').

244 See, eg, Greenleaf, Waters and Bygrave, above n 65; Graham Greenleaf, Nigel Waters and Lee Bygrave, Submission to the Australian Law Reform Commission, *Review of Privacy Issues Paper No 31,* January 2007, 524. The ALRC considered the Privacy Commissioner's reporting, particularly in regard to its OMI reports, and recommended that it could be more comprehensive, particularly in regard to the specific details of investigation outcomes. See *For your information* above n 32, [50.17].

other than where a determination is made.[245] In the absence of a specific legislative provision to that effect, the Australian common law does not require the Commissioner to provide reasons for its decisions.[246] However, there are recognised issues where decision-makers provide either no reasons, or inadequate reasons. These include that:

- Business lacks certainty about how to comply with the law;
- Potential complainants or respondents (or their professional advisers) have very little information about how the Act is interpreted by the Commissioner, and little idea what arguments they need to raise;
- Scholars are hampered in the development of privacy jurisprudence, because without decisions they have no basis for a critical analysis of how the Commissioner is interpreting the Act;
- The ability of the press, consumer organisations and privacy advocates to keep watch on the adequacy or fairness of Privacy Commissioners' decisions and remedies is impeded; and
- Privacy Commissioners are able to 'bury their mistakes', so that any misinterpretations of the law, and any failures to insist that government agencies and business interests provide adequate remedies in individual cases, are less likely to come to light. [247]

Notwithstanding that there is no obligation do so, there is evidence that the OAIC intends that its published case notes and OMI reports provide adequate reasons for decisions, at least to the extent that that can be regarded as an integral part of the transparency of decision-making.

---

245 *Privacy Act* s 55(2).

246 See the High Court in *Public Service Board (NSW) v Osmond* (1986) 159 CLR 656, which held that an administrative decision-maker had no obligation at common law to give reasons for a decision. Other commentators have suggested more recently that it is time for the common law position in Australia to change, as it has in Canada and the United Kingdom. See Justice Chris Maxwell, 'Is the giving of reasons for administrative decisions a question of natural justice?' (2013) 20 *Australian Journal of Administrative Law* 76; and Justice Mark Weinberg, *Adequate, Sufficient and Excessive Reasons* (Judicial College of Victoria, 2014).

247 Greenleaf, above n 65.

The OAIC has said that case notes are produced 'to demonstrate transparency of decision-making.'[248] The OAIC's *Guide to Producing Case Notes* states that it is intended that published reports will illustrate the application of the privacy principles in common circumstances, the OAIC's interpretation of the Act or the OAIC's complaint-handling process in relation to complex or difficult investigations.[249] Similar statements are included on the OAIC's website.[250] The Commissioner has said that the publishing of investigation reports will provide 'a public record of the OAIC's views on how privacy laws should be interpreted,' which can 'assist complainants and respondents to better understand how privacy laws will apply' and increase 'transparency in our investigation process and … help organisations and agencies to better understand their privacy responsibilities.'[251]

The role of OMI reports in providing transparency of decision-making was referred to by the OAIC in its response to one of the FOI applications made as part of this research. In considering whether to provide access in the interests of enhanced scrutiny of public decision-making, the OAIC decision-maker (determining largely not to provide that access) noted that the access was not necessary as '(t)he purpose of the OMI report is to provide the public with the necessary information to scrutinise the decision-making process.'[252]

---

248 See, eg, *OAIC 2011 Annual Report*, above n 1, 38.

249 Office of the Australian Information Commissioner, 'Guide to Producing case notes' (January 2013) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/guide-to-producing-case-notes > ('*Guide to Producing Case Notes*').

250 Office of the Australian Information Commissioner, 'Privacy case notes' (12 April 2013) <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-case-notes>. Case notes are also published on AustLII, <http://www.austlii.edu.au/au/cases/cth/AICmrCN/>. Case notes of privacy matters finalised by the former Office of the Privacy Commissioner are published at Office of theAustralian Information Commissioner, 'Privacy case notes – archive' <http://www.oaic.gov.au/privacy/privacy-archive/privacy-case-notes-archive/>.

251 Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy law reform: challenges and opportunities' (Paper presented at the Emerging Challenges in Privacy Law Conference, 23 February 2012) <http://www.oaic.gov.au/news/speeches/timothy_pilgrim/timothy_pilgrim_emerging_challenges_feb12.html#_ftn1>.

252 Ultimately it was determined that access would be denied as the public interest mattes were outweighed by 'the potential for commercial damage to the third party organisations and

To illustrate and promote a better understanding of the application of privacy principles, it would be expected that the Commissioner's published case notes and OMI reports would provide a clear explanation of the way the principles have been interpreted and applied in the particular circumstances. Similarly, it would be expected that that explanation would be supported by clear and logical reasons for the decision, grounded in findings of fact that are supported by the evidence. Clarity of reasoning, based on facts that support the decision made, are all part of transparency of decision-making.

Recently, the OAIC has issued a draft *Regulatory Action Policy*[253] for consultation. This draft policy provides that, when making decisions, the OAIC will act consistently with general principles of good decision-making, as explained in the ARC's *Best Practice Guides*, which include *ARC Best Practice Guide 4 - Reasons*[254] (the '*ARC Decision Guide'*). The *ARC Decision Guide* states that providing reasons for a decision 'aligns with other important principles of administrative law that require accountability and transparency in decision- making.'[255]

In determining whether the reports to be analysed later in this research meet the requirements for good decision-making, as part of the overarching principle of transparency, this research will use the direction included in the *ARC Decision Guide*.[256] This *Guide* provides that reports should detail all the steps in the reasoning process, linking the facts to the decision such that a reader should be able to understand exactly how the decision was reached without having to guess at any gaps.[257] To achieve this, the *ARC Decision Guide* provides that decisions should clearly contain the following:

---

potential impediment to information exchange between the OAIC and third party organisations in the future.' Letter from Caren Whip, Office of the Australian Information Commissioner to Jodie Siganto, 30 August 2013.

253 *Regulatory Powers Policy*, above n 227.

254 *ARC Decision Guide*, above n 243.

255 Ibid 2.

256 *ARC Decision Guide*, above n 243.

257 Ibid 8 – 9.

- The decision, referring to the legislation that authorised the decision, the relevant statutory provision and those aspects which need to be resolved or answered, and the decision reached on those matters;
- The findings on material facts, which should include all material facts. When a finding of fact is inferred, the statement should set out the primary facts and the process of inference;
- The evidence or other material on which those findings are based. This should include all evidence that was considered relevant, credible and significant in relation to each material finding of fact. The statement should demonstrate that each finding of fact is rationally based on evidence; and
- The reasons for the decision, detailing all the steps in the reasoning process that led to the decision, linking the facts to the decision.[258]

The analysis of the published reports included in this research will consider the extent to which those reports meet the above criteria to determine whether they comply with the principles of good decision-making, in addition to the elements of procedural fairness. This in turn will influence the extent to which the Commissioner's reports can be regarded as transparent.

## 2.7 CONCLUSION

Australia's *Privacy Act* is based on the *OECD Privacy Guidelines* and included a principle, known as NPP 4, which required that organisations take 'reasonable steps' to protect personal information from misuse and loss and unauthorised access, modification and disclosure. Similar principles form part of other privacy regimes.

The *Privacy Act* is based on two regulatory approaches: principles rather than rules as the basis for regulation and a responsive regulatory approach to compliance. For the purposes of this research, the main consequences of those regulatory foundations are:

---

[258] Ibid 7 – 9.

- The need for active engagement between the Commissioner as regulator and the regulated community to develop a shared understanding of what outcomes are intended by those principles and how they should be met, given the uncertainty of the wording of the principles; and
- In terms of compliance, the use by the regulator of a wide range of oversight and investigation powers to achieve compliance in a responsive rather than a punitive way, with a focus on guidance and education.

Consistent with the regulatory foundations of the Act, the Commissioner holds a wide range of powers which fall into two categories:

- Oversight powers, including powers to monitor developments and undertake research, advise, audit, educate and issue binding and non-binding guidance; and
- Investigation powers, including the power to carry out complaint-based and own motion investigations and to make determinations.

The ALRC noted that it was important, given the broad range of powers available and the legislative reliance on a responsive regulatory approach, that the Commissioner exercise those powers in a way that could be regarded as transparent, balanced and vigorous. These principles are broadly consistent with those proposed by other regulators and commentators for the effective exercise of regulatory powers. Accordingly, it is proposed that for the purposes of this research the appropriateness of the Commissioner's use of both its oversight and its investigation powers will be assessed by reference to principles of transparency, balance and vigour. It was also noted that the idea of transparency had further facets when considered in the context of the use of the investigation powers. In particular, it was noted that, as part of the need to provide transparency, investigations and decisions should be made in accordance with the principles of procedural fairness and the right to receive adequate reasons for a decision. When considering the adequacy of the evidence (as part of the consideration of procedural fairness), this research will consider whether:

- All material questions of fact have been determined;
- Every decision on a fact is based on evidence for that fact; and

- Every finding of fact is based on evidence that is relevant and that logically supports the finding.[259]

When considering whether adequate reasons for a decision have been given in a report, this research will consider the following:

- Does the decision refer to the legislation that authorised the decision, the relevant statutory provision and those aspects which need to be resolved or answered, and the decision reached on those matters;
- Are clear findings made on all material facts;
- Does the report refer to the evidence or other material on which those findings are based and is that finding of fact rationally based on evidence; and
- Do the reasons for the decision link the facts to the decision?[260]

All of these considerations will form part of the conceptual framework to be used in the analysis of the Commissioner's use of its oversight and investigation powers to answer the third sub-question: To what extent is the exercise of those powers consistent with principles for the exercise of regulatory powers?

The next chapter will consider information security best practice in Australia, in order to assist in answering the second sub-question: What is the relationship, if any, between the exercise of those powers and recognised industry practice in Australia?

---

259 *ARC Evdence Guide*, above n 237, 1.

260 *ARC Decision Guide,* above n 242.

# Chapter 3: Information Security

## 3.1 INTRODUCTION

Although there is ample evidence of information security failures with the almost daily publication of details of new data breaches, there is only limited understanding outside the world of information security specialists of what is meant by information security and why it is so challenging. This chapter will define 'information security' and explore the complexities of securing data by reference to the development of computing and data network technology.[261] It will then consider how the desired outcomes of information security can best be met, by reviewing current industry practices and standards. From this, a framework for an industry practice approach to information security will be derived. This framework will be used to answer the second sub-research question: What is the relationship between the Commissioner's exercise of his investigation and oversight powers and recognised industry practice in Australia?

## 3.2 DEFINITION OF 'INFORMATION SECURITY'

Generally, the term 'security' is understood to mean the protection from threats.[262] The most commonly used definition of information security is 'the preservation of confidentiality, integrity and availability of information' [263] where:

---

261 'Definitions and characterisations are significant because our view of information security and its management is greatly influenced by the definitions and the frameworks through which we categorise and sort the different contexts that we seek to secure.' Lizzie Coles-Kemp, 'Information security management: An entangled research challenge' (2009) 14(4) *Information Security Technical Report* 181

262 Smedinghoff, above n77.

263 This is the definition used in *ISO 27001*, above n 48. See also T Peltier, 'Establishing business control for electronic mail communications' (1998) 12 *Information Systems Security* 34; M Krauss and H Tipton, *Handbook of Information Security Management* (CRC Press, Boca Raton, Florida, 2012); Meints, above n 71.

- ‘Confidentiality’ is the property that information is not made available or disclosed to unauthorised individuals, entities or processes;[264]
- ’Integrity’ means ‘the property of protecting the accuracy and completeness of records,’[265] and
- ‘Availability’ is ‘the property of being accessible and usable upon demand by an authorised entity’.[266]

This definition is based on identifying the objectives of information security, which also include accountability, non-repudiation and authentication.[267] Another definition, from the perspective of how security is to be achieved (rather than by describing security by the desired outcomes) is:

> Security is a combination of physical, logical (ICT) and personnel security measures designed and implemented to provide ‘defence in depth’ appropriate to the perceived threats/risks to the assets being secured.[268]

The need to combine a range of different measures to ensure the confidentiality, integrity and availability of information is a consequence of the way that computer technology and computer networking (via both private networks and public networks such as the internet) has developed and been adopted by government, private enterprises and individuals.

## 3.3 BACKGROUND

The first electronic computers were developed during and immediately following World War II.[269] These were largely stand-alone systems housed on

---

264 International Standards Organisation, *ISO/IEC 27000:2014 Information technology — Security techniques — Information security management systems — Overview and vocabulary*, (2014), 2 (‘*ISO 27000’*).

265 Ibid 5.

266 Ibid 2.

267 Qingxiong Ma, Allen C Johnston and J Michael Pearson, 'Information Security Managegement Objectives and Practices: A Parsimonous Framework' (2008) 16(3) *Information Management & Computer Security* 251.

268 Australian Government Information Management Office, *Commercial Service Provider Assurance Framework* (Department of Finance, September 2012).

government premises and were used to run a single program at a time. The main security risk was unauthorised access, which could be prevented by both physically securing the machines and limiting physical access to a small group of known authorised operatives.[270] Developments such as the sharing of processing on the same system (with different people performing different tasks) introduced new risks by, for example, making it possible for one user to read and modify another user's data.[271] As a result, logical access controls (such as user identification and authentication) were incorporated into computing technology.

As computers became cheaper and the benefits from automating processes became more widely understood, computers moved out of the defence and research world and into mainstream government and business use.[272] These computers were still largely stand-alone machines that could be physically protected from unauthorised access, although the business requirements for the integrity of processing and availability of both the data and the data processing systems introduced new 'security' issues.

The increasing general use of computers also saw new threats, with the first computer viruses appearing in the early 1980s, spread by diskettes, which at that time were the principal method for transferring information between physically remote

---

269 See, for example, William T Moye, 'ENIAC: The Army-Sponsored Revolution' (<http://ftp.arl.army.mil/~mike/comphist/96summary/>; *John W. Mauchly and the Development of the ENIAC Computer* <http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html > and 'Introduction to the Mark 1' <http://www.computer50.org/mark1/mark1intro.html>.

270 See Whitfield Diffie, 'Information Security: 50 years Behind, 50 Years Ahead' (2008) 51(1) *Association for Computing Machinery. Communications of the ACM* 55; and Jeffrey Yost, 'A History of Computer Security Standards' in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007) 595, 599.

271 Ibid Diffie, 55: 'The turn from the 1960s to the 1970s marked the birth of both computer security and the modern era in cryptography.' Time-sharing was one of the main areas of research supported by the United States Government's Advanced Research Project Agency's ('ARPA') Information Processing Technique's Office; M T Dlamini, J H P Eloff and M M Eloff, 'Information security: The moving target' (2009) 28(3-4) *Computers & Security* 189, 189-198.

272 Margaret van Biene-Hershey, 'IT Security and IT Audting Betwen 1960 and 2000' in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007), 665.

and unconnected computer systems.[273] Concerns around the spread of viruses highlighted the risks posed by untrained employees as well as the vulnerability of most systems to malicious software.[274] The need for anti-virus software as well as appropriate training for any personnel who had access to computing equipment was added to other existing security measures: logical access controls, physical security and secure technology.

The inefficiencies of exchanging information via diskettes were increasingly overcome by linking computers by networks, usually established using phone lines.[275] These original networks were largely based on proprietary hardware and software (such as IBMs SNA)[276,] which made it difficult to establish connections between different types of computer systems.[277] In the 1990s, to overcome the restrictions of proprietary networking technology, organisations started moving to the ARPANET network, the use of which until then had largely been limited to the government and research institutions.[278] ARPANET was based on a non-proprietary protocol for transmitting data: TCP/IP.[279] TCP/IP, still used today, supports the transmission of data packets 'in the clear.' This means (in the simplest sense) that data packets travelling across the network can be intercepted and read by anyone who can access any part of the network on which the packets are being transmitted.

---

273 'Elk Cloner' and 'The Brain' are reported to be among the first viruses ever created. D PJ Denning, *Computers under attack: intruders, worms, and viruses* (Addison-Wesley Publishing Company, United States of America, 1991).

274 See, eg, Fred Cohen 'On the implication of computer viruses and methods of defense' (1988) 7(2) *Computers & Security Journal* 167.

275 Laura DeNardis, 'A History of Internet Security', in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), above n 271.

276 See H. Gilbert, *Introduction to SNA* (2 February 1995) <http://www.yale.edu/pclt/COMM/SNA.HTM>.

277 Margaret van Biene-Hershey, above n 271, 664.

278 The APRA NET network had been developed by the ARPA, as part of a U.S. Department of Defense funded project to produce a redundant, reliable network which remote mainframes could use to communicate data in the event of a nuclear attack. It was a response to United States' concerns that it was trailing the Soviet Union in scientific research following their launching of the Sputnik (which justified the significant investment in research at the time), and a desire to ensure the preservation of command and control communications capability in the event of a nuclear attack. See Laura DeNardis, above n 274, 682.

279 Ibid. "TCP/IP" means transmission control protocol and internet protocol.

TCP/IP provides interoperability, flexibility and rout-ability but is an inherently insecure protocol.[280] However, it remains the most commonly used protocol for the transmission of data, with the transformation of ARPANET into the internet following the development of another new protocol developed in the late 1980s, HTTP.[281] The adoption of TCP/IP led to a range of security add-ons to help protect data in transmission, such as encryption, as well as new architectures incorporating elements such as firewalls and de-militarised zones, to protect organisations from malicious network traffic entering and compromising their systems. The new interconnectedness via the internet provided an easy vector for attack by a vast range of adversaries against any government, organisation or individual connected to the ubiquitous network. It led to a whole set of new security issues, such as website defacements, botnets and denial of service attacks, caused by malicious actors. The potential for the large-scale disclosure or compromising of information as a result of an accident or unintentional human error increased.

Challenges for securing computers and the information that they processed had been recognised as early as the 1960s.[282] A project to investigate security issues funded by the US government resulted in a report issued in the early 1970s by the US Department of Defense titled *Security Controls for Computer Systems*, also known as *The RAND Report*.[283] It recognised that computers would be the product of private industry, not the government, and explicitly called for a shift away from thinking of security purely in terms of a technology problem and hardware protection (or computer security) to conceiving of it more in terms of data, users, and

---

280 Andrew G Blank, *TCP/IP Foundations* (Sybex, Alameda, USA, 2004) 2-3.

281 HTTP (hyper-text-transfer-protocol) supports hyperlinked pages of information distributed over the internet and was invented in 1989 by Tim Berners-Lee, an academic looking to support academic research sharing. It is the foundation of data communication on the world wide web.

282 See, eg, the quote from Willis Ware, one of the early computer security leaders and the man responsible for the Rand Report (referred to below) from Jeffrey Yost, above n 270, 601.

283 The Rand Report was produced as a result of a Task Force organized by ARPA in 1967 to study and recommend appropriate computer security safeguards that would protect classified information in multi-access, resource-sharing computer systems. The Rand Corporation, *Rand Report R-609*, *Security Controls for Computer Systems* (Department of Defense, February 1970) <http://www.rand.org/pubs/reports/R609-1/index2.html> ('The RAND Report').

infrastructure. The approach recommended in the *RAND Report*, which was based on a combination of administrative, technical and procedural security measures to manage the technology and the people who interact with it, has influenced the subsequent development of information security practice and is reflected in most of the current approaches to information security. Accordingly, the *RAND Report* is regarded by many as the seminal document for computer security.[284]

## 3.4 INFORMATION SECURITY BEST PRACTICE

As a consequence of the development of computing and networking technology, there is no simple solution to information security. What is required is a combination of administrative, technical and procedural security measures to manage the technology and the people who interact with it. For the purposes of this research, it is important to understand whether there exists a broadly accepted approach to ensuring information security that may be used as the standard or benchmark for determining whether reasonable steps were taken to protect personal information for the purposes of NPP 4.

Consideration of the different industry approaches to information security in the literature has been limited almost exclusively to technical issues.[285] The major information security standards have been compared and the parallels between them noted; however, there has been little detailed assessment of their relative strengths and weaknesses or whether they all support a generally similar approach.[286] There has certainly been only limited consideration of information security standards in the legal context.[287]

---

284 Ibid.

285 The absence of any extensive non-technical research into information security standards has been noted. In particular, the need for more interdisciplinary review of information security, especially by reference to psychology and sociology theories, has been identified. See, for example, Coles-Kemp, above n 260.

286 See, eg, H Susanto, M Nabil Almunawar and Yong Chee Tuan, 'Information Security Management System Standards: A Comparative Study of the Big Five' (2011) 11 *International Journal of Electrical and Computer Sciences* 23; and Constantine Gikas, 'A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards' (2010) 19(3) *Information Security Journal: A Global Perspective* 9.

287 See, eg, Gifford, above n 44.

The following describes the most widely used of the different approaches to information security in Australia and internationally.

### 3.4.1 General Information Security Standards

#### 3.4.1.1 ISO 27001 Information Security Management System

The International Standards Organisation (ISO)[288] publishes standards which are said to represent a consensus on current practice. They are developed following a period of public enquiry and consultation, including with consumers, academia, special interest groups, government, business and industry. They are designed for voluntary use, although they may be adopted by industry or imposed by governments. ISO 27001[289] and ISO 27002,[290] both issued by ISO have been referred to as 'the closest thing to a universal information security standard.'[291] These standards were referred to as the benchmark for reasonable security in those Australian texts that have considered the issue.[292]

As at March 2014, the range of ISO standards relating to information security includes ISO 27001, ISO 27002 and ISO 27005.[293] These international standards have been reviewed and approved for release in Australia.[294]

ISO 27001 provides the specification for an information security management system (ISMS) against which certification by an ISO Certification body, based on the recommendation of an authorised third party auditor, can be granted. The objective

---

288 ISO is a nongovernmental body, made up of representative bodies from over 160 countries.

289 *ISO 27001*, above n 48.

290 *ISO 27002*, above n 49.

291 Gifford, above n 44, 193 - 194

292 See Chapter 1.5.1 for consideration of the relevant literature.

293 International Standards Organisation, *ISO/IEC 27005: 2008 Information Technology – Security techniques - Information Security Risk Management* (2005) ('*ISO 27005*'). For more information on the ISO 27000 series of standards refer to the following website: <http://www.27000.org/iso-27005.htm>.

294 The Joint Technical Committee IT-012 whose members include Commonwealth Attorney General's Department, ABA, IIA, DOD, AEEMA and the Certification Forum of Australia, approves internationals standards for adoption in Australia.

of the standard itself is to 'provide a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an Information Security Management System.' [295]

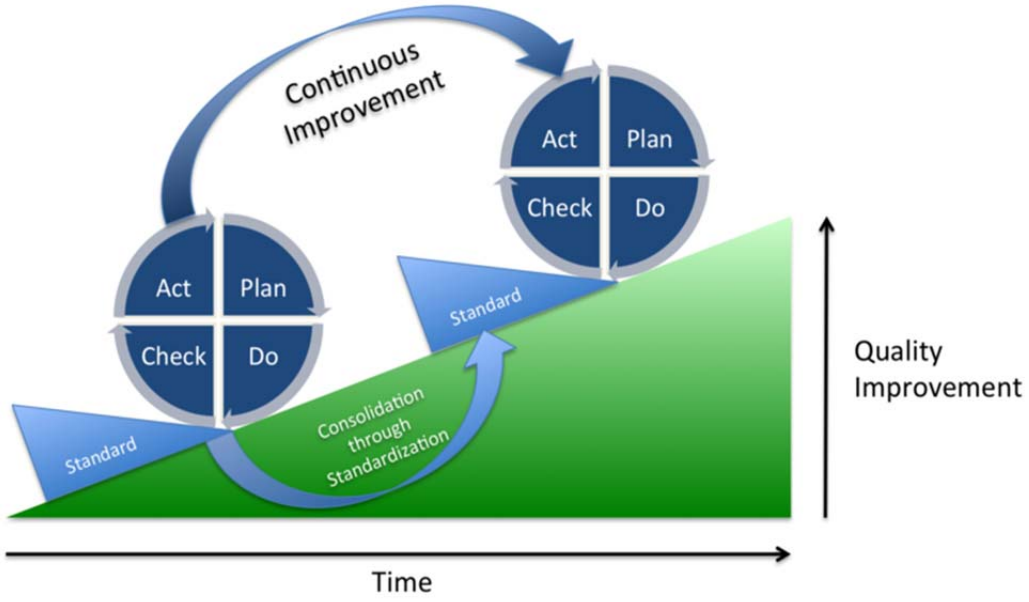



*Figure 3: Plan Do Check Act model*

The management model proposed by ISO 27001 adopts a continual improvement cycle, which means that an organisation needs to regularly monitor and review the effectiveness and performance of its ISMS and to make improvements as necessary to ensure it maintains the desired level of protection.[296] An example of this continuous improvement cycle is the Plan Do Check Act Model shown in *Figure 4*.

ISO 27001 uses risk management as the basis for the selection of controls and for the review of the effectiveness and performance of the system. After identifying the assets that are within the system, an assessment of the information security risks

---

295 *ISO 27001* above n 48, v.

296 This process design is often referred to as the Deming Cycle, which has been established in the context of quality of management for more than 50 years. The same process model is used by other ISO management standards such as ISO 9001 (Quality Management System), ISO 14001 (Environmental Management System) and ISO/IEC 20000-1 (IT Service Management).

to those assets is undertaken. 'Information security risk' is defined in ISO 27005 as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm.[297]

Once the risks have been assessed and prioritised for action, a system of controls must be selected to 'manage' those risks. The controls, which must be customised to the needs of each individual organisation within the context of an organisation's overall business risks, should be selected from all sources then compared to the list in ISO 27001 Annex A and ISO 27002 for the sake of completeness.[298]

ISO 27001 Annex A and ISO 27002 contains 14 control areas and 114 separate controls. The 14 control areas are:

- Security policy;
- Organisation of information security;
- Asset management (which includes classification);
- Human resources security;
- Physical and environmental security;
- Operations management;
- Access controls;
- Cryptographic controls;
- Information systems acquisition, development and maintenance;
- Communications security;
- Supplier management;
- Information security incident management;

---

297 *ISO 27005*, above n 293, 1.

298 *ISO 27001*, above n 48, 4. See also Gikas, above n 285.

- Business continuity management; and
- Compliance.

ISO 27001 is the most commonly referred to information security standard, but it is not without its critics.[299] Criticisms include that the standard is outdated (it is based on an approach to security management and a body of text created over twenty years ago),[300] that the focus on outputs supports the perception that the standard can be applied 'mechanistically'[301] and that it fails to recognise the importance of specific organisational and societal factors.[302]

Other international standards relevant to information security, in addition to the ISO 27000 series of standards, are detailed below.

#### 3.4.1.2 OECD guidelines for the security of information systems and networks

The Organisation for Economic Co-operation and Development (OECD) first published guidelines for the security of information systems and networks in 1992.[303] They were updated and reissued in 2002 as part of the five-yearly review cycles.[304]

---

299 Cath Everett, 'Is ISO 27001 worth it?' (2011) 2011(1) *Computer Fraud & Security* 5; and Alan Gillies, 'Improving the quality of information security management systems with ISO 27000' (2011) 23(4) *The TQM Journal* 367, which examines the barriers to adoption of ISO 27001 and refers to costs, particularly those of consultants as one of the issues.

300 David Lacey, 'Security: Best practice or ancient ritual?' *ComputerWorld UK* (online), 12 January 2011<http://www.computerworlduk.com/in-depth/security/3256436/security-best-practice-or-ancient-ritual/#>.

301 The validity of the guidelines by appeal to common practice has also been questioned. See Mikko Siponen and Robert Willison, 'Information security management standards: Problems and solutions' (2009) 46(5) *Information & Management* 267.

302 Coles-Kemp, above n 260. But also see, eg, R Werlinger, K Hawkey and K Beznosov, 'An integrated view of human, organizational, and technological challenges of IT security management' (2009) 17(1) *Information Management & Computer Security* 4, which undertakes a study to determine the main challenges that IT security practitioners face in their organizations, including the interplay among human, organizational and technological factors.

303 Organisation for Economic Co-operation and Development *OECD Guidelines for the Security of Information Systems and Networks* Recommendation of the OECD Council at its 22nd Session on 14 – 15 October 1992 (OECD, 1992) <http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm.>. A review in 1997 determined that the Guidelines did not need to be updated at that time.

304 Organisation for Economic Co-operation and Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* Recommendation of the OECD Council at its 1037th Session on 25 July 2002

Driven by both the growing ubiquity of networks and the events of 11 September 2001,[305] the updated Guidelines recognised the increased interconnectivity of systems and consequently the need to develop a 'culture of security' which represented a new way 'of thinking and behaving when using and interacting within information systems and networks.'[306] The adoption of the 2002 Guidelines marked a switch from a 'risk avoidance' model for the security of previously isolated and siloed information systems, to a 'risk assessment and management' approach. There are clear parallels between the 2002 *OECD Security Guidelines* and the risk-based management system specified in ISO 27001. Both provide a framework for organisations to manage security issues in accordance with their own risk appetites. However, there is little consideration of external factors in the *OECD Security Guidelines*, although they do refer to basic principles such as acting ethically.

The OECD has also done important work around cryptography, recognising that the 'use of effective cryptography in a network environment can help protect the privacy of personal information and the secrecy of confidential information.'[307] The use of encryption to protect the confidentiality and integrity of information and also non-repudiation and authentication makes encryption an important security control.[308]

---

http://www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsaculture ofsecurity.htm ('*OECD Security Guidelines*'). See also Organisation for Economic Co-operation and Development, *Review of the 2002 Guidelines* (OCED, 2012) <http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf>, 35-36.

305 Organisation for Economic Cooperation and Development, *The Role of the 2002 Guidelines: Towards Cybersecurity for an Open and Interconnected Economy* (OECD Digital Economy Papers No 209, OECD Publishing, 2012 ) <http://dx.doi.org/10.1787/5k8zq930xr5j-en at 36>.

306 *OECD Security Guidelines*, above n 304

307 Organisation for Economic Cooperation and Development, *Recommendation of the Council concerning Guidelines for Cryptography Policy* 27 March 1997 - C(97)62/FINAL.

308 See, eg, Section 10 Cryptography of *ISO 27001*, above n 48, 14 which refers to the use of cryptographic controls 'to protect the confidentiality, authenticity and/or integrity of information.'

Unfortunately, though useful at a high level and supported by other publications, the *OECD Security Guidelines* do not offer the same level of detailed operational guidance as ISO 27001 or even CobiT, which is probably the second most widely used security management system. The 2002 *OECD Security Guidelines* are currently under review.[309]

#### 3.4.1.3 CobiT

A different approach to ISO 27001 is provided by CobiT (from 'Control Objectives for Information Technology'), which is a widely used management framework for information security. Developed by the Information Systems Audit and Control Association (ISACA), it is a non-technical framework that divides a list of suggested controls into four phases or domains dealing with 'Planning and Organisation (PO)', 'Acquisition and Implementation (AI)', 'Development and Support (DS)' and 'Monitoring and Evaluation (ME)'. It has a broader scope than ISO 27001 in that it is concerned with the governance of all information technology but, like ISO 27001, is concerned with an overall approach rather than the specification of granular procedures.[310] Similar to ISO 27002, CobiT contains a series of control recommendations that support the high level requirements (equating to the ISO 27001 system requirements). Information security controls recommended include, for example:

- Ensuring information security is managed at the highest level of the organisation and in line with business requirements;
- Identifying security requirements based on a risk analysis and compliance requirement and reflecting this as a documented set of policies and procedures; and
- Ensuring these are properly implemented and communicated to all users and shareholders.

---

309 Roger Clarke, *Challenges Facing the OECD's Revised Security Guidelines* (2013) <http://www.rogerclarke.com/SOS/OECDS-1311.html>.

310 Gifford, above n 44, 197.

CobiT is probably best thought of as a complementary system to the ISO 27001-based management system, providing additional support in the design of the management system through its governance and auditability focus.

#### 3.4.1.4 Payment Card Industry — Data Security Standard (PCI-DSS)

By contrast, the Payment Card Industry–Data Security Standard (PCI–DSS)[311] is a mixture of principles, guidance and prescriptive requirements backed up by a system of private incentives and penalties. The PCI-DSS was developed by the founding payment brands of the PCI Security Standards Council, including American Express, MasterCard Worldwide, and Visa Inc. International, to help improve the security of credit card holder data (and to reduce losses and reputational damages through fraudulent credit card usage.)

It is an example of an industry addressing its own data security needs. Compliance with the PCI-DSS is a matter of contract enforced between the credit card companies, the banks and the merchants. There is the possibility of significant penalties being imposed for failure to comply with the PCI-DSS if a breach of security occurs, together with termination of the right to process credit card payments, which operate as significant incentives for compliance by merchants and other organisations that process credit card payments.

The PCI-DSS provides a general set of security requirements that can be customised for each organisation, including requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. It is based on the implementation of 6 security principles that include 12 high-level security requirements, which are themselves supported by over 100 more detailed controls. The 6 principles are:

- Build and maintain a secure network;
- Protect cardholder data;

---

311 Payment Card Industry Security Standards Council, *Payment Card Industry Data Security Standard version 3.0*', 2013 <https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf>.

- Maintain a vulnerability management program;
- Implement strong access control measures;
- Regularly monitor and test networks; and
- Maintain an information security policy.

The standards specified in PCI-DSS are different to the 14 domains in ISO 27001 and the supporting controls in ISO 27002. The PCI-DSS principles are not sequential or linear and vary in nature, scope and granularity. 'Some ... are prescriptive while others ... are normative in the sense that they leave the particular means of implementing protection and security to the entity responsible for compliance.'[312]

In addition to specifying security standards, the PCI-DSS program includes requirements for regular third party testing and independent audits of compliance, depending on the number of transactions processed by merchants. The results of these audits must be submitted to the PCI-DSS Council on a regular basis. As stated, failure to comply can lead to fines and, ultimately, loss of the right to process credit card transactions. The mandatory monitoring of compliance with the standard by the PCI-DSS Council is one of the differentiators of this standard from ISO 27001, where certification of compliance by an independent auditor is a voluntary option.

### 3.4.2 Australia Government Information Security Management

Both the Federal and the State governments have developed approaches to secure the information held in government-controlled systems.

Australian Federal government agencies are covered by a specially designed framework comprised of the *Protective Security Policy Framework* (PSPF) [313] and

---

312 Edward A. Morse and Vasant Raval, 'PCI DSS: Payment card industry data security standards in context' (2008) 24(6) *Computer Law & Security Review* 540, 550 – 551.

313 The Commonwealth Attorney-General sets Government's protective security policy and has released the Protective Security Policy Framework, in pursuance of that responsibility. Attorney General, *Protective Security Policy Framework Securing Government business* (Attorney General's Department 2010) ('*PSPF*').

the *Information Security Manual* (ISM).[314] Although not binding on private organisations, these documents are of interest because they are stated to represent best practice in mitigating or minimising the threat to Australian government systems.[315]

The ISM is based on a series of high-level principles which are supported by a detailed controls manual. The first principle is information security risk management, which supports agencies making informed, risk-based decisions specific to their unique environments, circumstances and risk appetite (subject to the implementation of a number of controls which are stated to be mandatory).[316] The ISM defines risk as the chance of something happening that will affect objectives. Risk is measured in terms of event likelihood and consequence. [317] The other principles refer to:

- Roles and responsibilities;
- Information security documentation (including security policy);
- Information security monitoring;
- Physical security;
- Personnel security; and
- Communications infrastructure.[318]

---

314 The ISM is published by the Australian Signals Directorate pursuant to the *Intelligence Services Act* 2001 (Cth). It is made up of a number of different publications including *ISM Principles*, above n 8; Australian Signals Directorate, *Australian Government Information Security Manual - Controls* (April 2013) <http://www.asd.gov.au/publications/Information_Security_Manual_2014_Controls.pdf> ('*ISM Controls'*).

315 *ISM Principles*, above n 8, 12

316 An example of how the selection of controls would typically be couched as responsive to risk assessment outcomes is the first control objective specified in the Australian Government Information Security Manual: 'Agencies select and implement information security controls from the ISM as part of a formal risk management process.' *ISM Principles*, above n 8, 1.

317 *ISM Principles*, above n 8, 63.

318 Ibid 12 – 34.

In addition, there is a range of more technology-specific principles dealing with topics including product security, media security, software security, email security, network security and cryptography.[319]

The approach and content of the ISM is closely related to that of the two main international standards for information security, ISO 27001 and ISO 27002. Given this closeness, the ISM can be taken to represent the implied approval by the Australian Government of those standards generally as the preferred approach to information security management. As noted by the Victorian Government, which itself adopts the PSPF and the ISM for Victorian Government agencies, the PSPF and ISM are based on the ISO 27000-series standards and the ISM itself is a developed version of ISO 27002, offering a 'more substantive set of controls ... with qualitative and evidence-based control recommendations.'[320]

The Australian Prudential Regulation Authority (APRA), the regulator of Australia's financial services industry, is one of Australian's best known regulators, with a wide remit including banks, credit unions and superannuation funds.[321] In 2010 it published a *Prudential Practice Guide* on the management of security risk in information and information technology (IT) (PPG 234).[322] Similar to the ISM and the ISO 27001 risk-based approach to information security management, PPG 234 supports the development of an IT security risk framework, which is to be regularly reviewed to ensure compliance and effectiveness, using a principles-based approach to provide flexibility for compliance by regulated organisations. However, unlike

---

319 Ibid 37 – 60.

320 The Victorian Government standards include Victorian Government Chief Technology Advocate, *SEC POL 01 Information Security Management Policy - 2012 version 201* (Victorian Government CIO Council, 1 October 2012) < http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-POL-01-Information-Security-Management-Policy1.pd>, 2.

321 According to APRA's website, APRA oversees banks, credit unions, building societies, general insurance and reinsurance companies, life insurance, friendly societies, and most members of the superannuation industry. APRA is funded largely by the industries that it supervises. It was established on 1 July 1998. Australia Prudential Regulation Authority, 'About APRA' (7 January 2014) <http://www.apra.gov.au/AboutAPRA/Pages/Default.aspx>.

322 Australia Prudential Regulation Authority, *PPG 234 - Management of security risk in information and information technology* (1 February 2010) <http://www.apra.gov.au/CrossIndustry/Documents/PPG_PPG234_MSRIT_012010_v7.pdf> ('*PPG 234*').

ISO 27001 and ISO 27002, it identifies areas of risk specific to the institutions regulated by APRA where it expects that specific controls should be implemented, including:

- User training and awareness;
- Access control;
- IT asset life-cycle management;
- Monitoring and incident management process; and
- IT security reporting and assurance mechanism.

Although differing in the high level control areas which are identified, the broad approach of recommending a risk assessment framework for the selection and review of security controls is consistent with the information security management approach specified in ISO 27001.

The State Governments in Australia have adopted different approaches to ensuring the security of the information that they hold, however, they all reference ISO 27001 and ISO 27002 to some degree. The New South Wales Government has long supported compliance with ISO 27001 and IS0 27002. [323] The Queensland Government has re-issued a modified version of ISO 27001 as an 'information standard'[324] and the Victorian Government in 2012 adopted the Commonwealth

---

323 In 2001, NSW Premiers Circular No. 2001 – 46 required agencies 'to have their IT systems certified to the national standard AS/NZS 4444 information security management when accredited certifiers become available' (see Premier and Cabinet, *M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations*. (NSW Government, 2001). This advice was updated by NSW Government's *Digital Information Security Policy 2012* covering the NSW public sector (Premier and Cabinet, *MD2012-15 Digitial Informatin Security Policy* (NSW Government, November 2012) < http://www.dpc.nsw.gov.au/__data/assets/pdf_file/0006/146688/Digital_Information_Security_Policy_2012.pdf> , 4 - 6 The Policy expressly refers to ISO 27001 and ISO 27002, including the requirement to have a risk based ISMS in place that incorporates a minimum set of controls. Organisations covered by the policy must be independently certified to be compliant with ISO 27001 (as from June 30, 2014), they must also provide an annual attestation to compliance as part of the body's annual report (from June 30, 2014). .

324 Queensland Chief Information Office, *Queensland Government Information Standard 18: Information Security*, (Department of Science, Information Technology, Innovation and the

Government's PSPF and ISM, which both incorporate the fundamentals of ISO 27001 and ISO 27002.[325]

### 3.4.3 Best practices approach to information security

The most prominent Australian government and regulator guidance and industry standards relating to information security have been briefly reviewed. The next question is whether any general propositions that could be used as the basis for describing a methodology for determining objectively what is reasonable in terms of securing personal information for the purposes of NPP 4 can be derived from those different approaches.

The comparison of the different approaches indicates that they all incorporate risk assessment to some extent together with some sort of iterative process-based management approach (including monitoring and review).[326] Accordingly, these two elements should be included in any 'standard' approach to information security management.

There is not as great a commonality in terms of the different types of security controls that are recommended to be implemented to address identified risks, although there is significant overlap. Further review of the different standards suggests that the most commonly recommended categories of security controls are:

- Personnel security (including training and user awareness);
- Physical security;
- Access controls;

---

Arts, December 2012) < http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy>.

325 Victorian Government standards include Victorian Government Chief Technology Advocate, *SEC STD 01 Information Security Management Framework version 3.1* (Victorian Government CIO Council, 1 October 2012) < http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-STD-01-Information-Security-Management-Framework.pdf>.

326 The need for a process in addition to risk is recognised outside the information security management standards, see e.g., K Bamberger, 'Technologies of Compliance: Risk and Regulation in the Digital Age' (March 2010) 88(4) *Texas Law Review* 815, 816; Kevin Cronin, 'Best Practice and the State of Information Security ' (2010) 84 *Chicago-Kent Law Review* 8. It has been suggested that a process based approach is part of the legal duty to take reasonable care to secure date in the United States: Smedinghoff, above n 77.

- Communications and network security;
- Information systems acquisition, maintenance and development; and
- Compliance.

Within each of these controls areas, different standards recommend different controls, with different degrees of specificity. Most approaches do not require the implementation of any particular control although there are some that are more prescriptive, such as the ISM and PCI-DSS. Given the earlier discussion about the complexities of information security and the need for multi-layered levels of defence, it is not surprising that most of the standard approaches to information security are not prescriptive regarding the specific controls that need to be in place, and refer instead to general domains where controls should be considered. This is a consequence of the determination of the detailed types of controls to be implemented being an outcome of the risk assessment process, rather than a mandatory requirement. As already mentioned, all the main standards (even those that include some mandatory controls such as the ISM and the PCI DSS) incorporate some reference to the need for a risk-based framework for the identification and implementation of security measures as part of an overarching information security management system. Accordingly, it could be said that general industry practice does not require that any particular security controls necessarily are in place, but it does suggest a range of different domains from which controls should be selected as part of a defence in-depth approach.

In summary, it is contended that there is a standard practice approach to information security, which is comprised of three interlinking components:

- The use of risk assessment as the basis for the identification of risks to assets and for the selection of security safeguards to manage that risk. The risk identification process should include the consideration of threats and vulnerabilities;
- The selection of security safeguards, including administrative controls (such as policies and personnel-related controls), physical and technical security

controls to manage the risks identified as part of the risk assessment and of the recurring process of review and re-calibration of the security system; and

- The adoption of an iterative monitoring, review and improvement process that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks.

#### 3.4.3.1 Information security and risk management

Given the importance of risk assessment and of an iterative management process to this standard practice approach to information security, it is appropriate to consider information security risk management in more detail.

Information security risk management is the overall process that integrates the identification and analysis of information security risks to which an organisation is exposed, the assessment of the potential impact on the organisation, and the decision regarding the action to be taken to accept, eliminate or reduce the risk to an acceptable level. It requires a comprehensive identification and evaluation of the organisation's information assets, the identification of risks to those assets (based on vulnerabilities and threats), the likelihood of occurrence and the consequences of those risks, and an assessment of the different risk treatments.[327]

The typical risk management process is illustrated by the flowchart in *Figure 4*, and incorporates the following:

- Risk assessment;
- Risk treatment; and
- Risk acceptance.

---

[327] Kevin J. Soo Hoo, *How much is enough? A risk-management approach to computer security* (Working Paper, Stanford University, CA, 2000) <http://iis-db.stanford.edu/pubs/11900/soohoo.pdf.> See also CISA, *CISA Review Manual 2006*, ISACA 2006. See also *ISO 27001*, above n 48, Section 4.2.1(d) which requires the identification of threats and vulnerabilities to organisational assets as part of establishing an ISMS

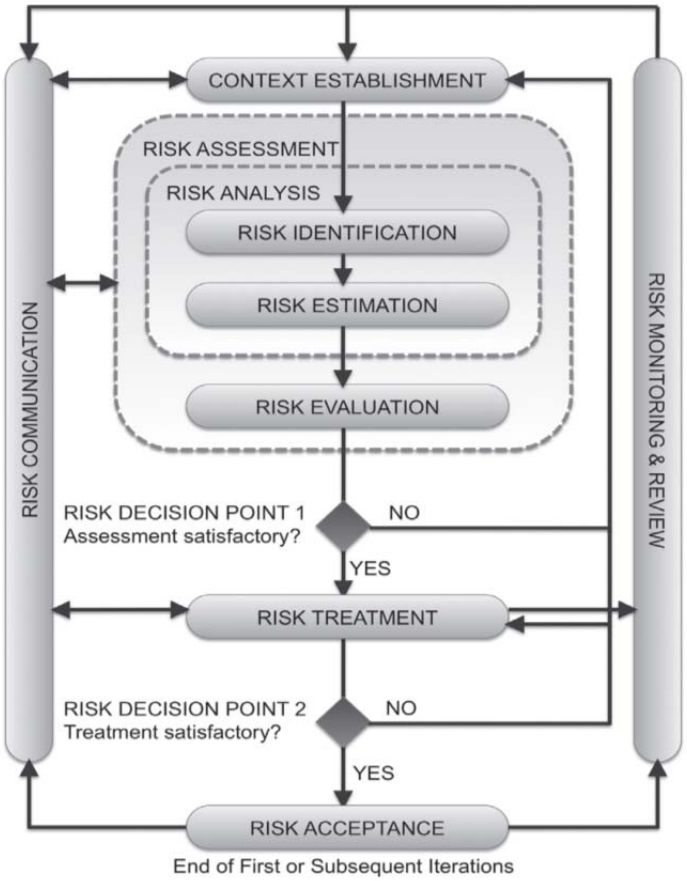



*Figure 4: Standard risk management process*

Risk assessment is the first step in the risk management process and is itself made up of the following steps:

- Risk identification;
- Risk estimation; and
- Risk evaluation.

For the purposes of this research, it is the process of risk assessment and treatment that is the most important because these set the objective standard that should be applied in particular circumstances.

### 3.4.3.2 Risk identification and evaluation

Information security risk assessment is different to other risk assessment in that it incorporates the actual identification of risks. ISO 27005 defines 'information security risk' as the potential for a threat to exploit a vulnerability, and notes that it is

measured in terms of a combination of the likelihood of an event and its consequences.[328] A threat is only worth considering if there is a vulnerability that can be exploited by the threat. Information security risks are identified through a consideration of threats and the weaknesses they may be able to exploit. Reflecting this relationship between threat and vulnerability, information security risks are often described by the following formula:

*Risk = Threat x Vulnerability*[329]

Accordingly, the identification of threats and vulnerabilities is a key part of information security risk assessment.

Threat source is an important consideration when identifying possible threats. Sources include:

- Human acts — intentional and accidental;
- Technical failure; and
- Physical and environmental factors (including fire, storm and flood).

Vulnerabilities are weaknesses which may be exploited by a threat. Examples of vulnerabilities include unpatched software, weak passwords, databases with limited access controls in place and the ability to connect unprotected devices to a network. Having identified a risk in terms of a threat and an exploitable vulnerability, the likelihood of that risk occurring is then assessed, as is an evaluation of the harm that will be caused if the risk occurs.

Risk assessment generally, and information security risk assessment in particular, is a complex area. For the purposes of this research, however, further consideration of information security risk assessment is not undertaken. The key

---

328 *ISO 27005*, above n 293, 1.

329 *ISO 27005*, above n 293, 10 - 13 refers to the identification of threats and vulnerabilities as part of the risk identification stage. National Information Assurance Training and Education Center defines risk in the IT field as 'the loss potential that exists as the result of threat-vulnerability pairs. Reducing either the threat or the vulnerability reduces the risk.' NIST SP 800-30 defines risk as 'a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation.' A more comprehensive definition of 'risk' that also included an evaluation of risk would also include consideration of the likelihood of occurrence and the impact if the risk did occur.

understanding is that risks must be identified and quantified, which is typically achieved by consideration of threats and vulnerabilities together with likelihood of occurrence and consequence, having regard to the particular circumstances of the organisation undertaking the assessment.

#### 3.4.3.3 Risk treatment

One of the main issues for effective risk treatment is the question of how to select the most 'appropriate' risk treatment once the risk has been identified. This is the third element of the standard approach to information security adopted by this research. Risk treatment options include avoidance, transfer, mitigation and acceptance. Mitigation is the most commonly used technique and is usually achieved by the selection of different security measures or 'controls.' Traditionally, risk treatments are selected on the basis of a cost-benefit analysis. However, this method of selection is being challenged by more sophisticated modelling, for example, the calculation of a perceived composite risk[330] or use of a quantitative analysis of different security measures that counteract individual risks by identifying information processes within an organisation (and the target security levels for all the identified core business processes) and the potential threats.[331] Whatever method is used, the outcome of the risk assessment phase will guide the risk treatment phase by informing:

- The type of security measure that should be in place, by reference to the nature of the risk, and the underlying threat and vulnerability pair; and
- The 'depth' of the controls that should be in place, which should be based on the level of risk.

For example, if the identified risk is the accidental disclosure of customers' personal financial records through the loss of back-up tapes, then the security

---

330 Lawrence D. Bodin, Lawrence A. Gordon and Martin P. Loeb, 'Information security and risk management' (2008) 51(4) *Communications of the ACM* 64.

331 Bojanc Rok Bojanc, Borka Jerman-Blažič and Metka Tekavčič, 'Managing the investment in information security technology by use of a quantitative modeling' (48) 6 *Information Processing & Management* , 1031.

measures that might be considered to reduce that risk could include back-up tape encryption, a defined process for the secure transfer of tapes to secure off-site storage locations, capability review of any third party involved in the transfer and off-site storage process and additional contractor and employee awareness training. The presence or absence of these controls, assessed in the context of the organisation's risk profile, should guide the determination of whether 'reasonable security' measures were in place. The type, number and extent of the controls that should be in place will be linked to the level of the evaluated risk in the specific circumstances, and the cost and ease of implementation of the relevant safeguards. Accordingly, it is difficult to assess the appropriateness of any security measure or system without an understanding of the specific risk environment.

It is worth reiterating that there is no silver bullet approach to information security. Effective security is based on interwoven measures covering people, processes and technology. This web of mutually supporting security controls is often referred to as 'defence in depth' where controls are selected and implemented in a layered model, building multiple defences as part of an interlocking system. The 'defence in depth' approach can be described the diagram in *Figure 3* below.

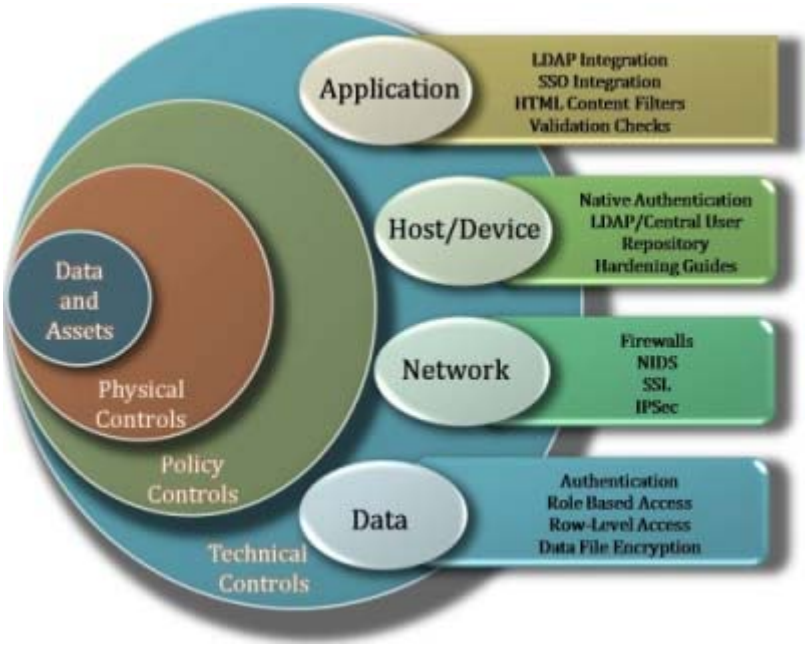


*Figure 5: Defence in depth*[332]

Although there are a number of recognised domains from which security measures can be selected, there is no single security control that, by itself, could be regarded as providing reasonable security. Conversely, the absence of a security control will not necessarily be fatal to the assessment of whether reasonable security measures have been taken. The answer will depend on both the specific risk environment and the other security controls in place.

The use of risk assessment as the underlying approach for information security management is not without issues. One of the problems is the absence of reliable data on the number and costs of attacks, intrusions and security breaches and the costs and the ease of implementing security controls. [333] Other issues include the different and personal perceptions of risk that make it difficult to use as an organisation-wide standard.[334] However, in the absence of more widely adopted approaches to information security management, this research will proceed on the basis that the standard practice is to use a risk-based approach.

## 3.5 CONCLUSION

In summary, information security practice is well developed although perhaps not well understood in the legal sphere. It is complex and challenging because of the inherent insecurities in the computer and networking technology used to collect, process, store and transmit electronic information, and the human interaction with that technology, and because of the wide range of threats to the confidentiality, integrity and availability of that information.

---

332 ARGis Resources, 'Security Principles' < http://resources.arcgis.com/en/communities/enterprise-gis/01n200000030000000.htm>.

333 Kathryn Picanso, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (October, 2006) 75 *FORDHAM L. REV.* 355, 360.

334 Hyeun-Suk Rhee, Young U. Ryu and Cheong-Tag Kim, 'Unrealistic optimism on information security management' (2012) 31(2) *Computers & Security* 221; C. Parker, 'Twenty years of responsive regulation: An appreciation and appraisal' (2013) 7 *Regulation & Governance* 2

Based on an analysis of common approaches to information security, it is contended that a standard practice approach to ensuring reasonable information security can be identified. This standard practice approach is comprised of three interlinking components:

- Risk: The use of risk assessment as the basis for the identification of risks to assets, and the selection of security safeguards to manage that risk. The risk identification process should include the consideration of threats and vulnerabilities;
- Security measures: The selection of security safeguards including administrative controls (such as policies and personnel-related controls), physical and technical security controls to manage both the risks identified as part of the risk assessment and the recurring process of review and re-calibration of the security system; and
- Process-based approach: The adoption of an iterative improvement process that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks.

This approach to information security practice will be used as part of the conceptual framework for the assessment of the exercise by the Commissioner of its powers in relation to industry practice. It will help answer the second sub-question: How has the Privacy Commissioner exercised its powers in regard to NPP 4 by reference to an industry practice approach to information security?

# Chapter 4: Method of Analysis and Data Collection

## 4.1 INTRODUCTION

The functions and powers available to the Commissioner were outlined in Chapter 2 as part of the broad consideration of the *Privacy Act* provisions. It was identified that the Commissioner's functions and powers included both oversight powers (such as monitoring, advice, audit, education and guidance) and investigation powers. The principles used to guide the exercise of those powers were then considered. It was determined that an appropriate lens for assessing the exercise by the Commissioner of those powers would be one that considered the extent to which that exercise could be regarded as transparent, balanced and vigorous. Accordingly, the principles of transparency, balance and vigour are used to answer the third sub-question posed in this research: To what extent is the exercise of the Commissioner's powers in regard to NPP 4 consistent with the principles for the exercise of regulatory powers?

A standard approach to information security that is based on an analysis of both industry and government approaches to information security was developed in Chapter 3. This approach is used as the second part of the conceptual framework for the analysis of the data in this research to help answer the second sub-question: How has the Privacy Commissioner exercised its powers in regard to NPP 4 by reference to an industry practice approach to information security?

The relationship between the two concepts forming the basis for the conceptual framework (that is, consistency with an industry practice approach to information security and the transparent, balanced and vigorous exercise of powers) and the overarching research question to be answered by this research (that is, how appropriate was the Commissioner's exercise of powers) is described in the diagram

included in *Figure 1: Framework to assess what is an appropriate regulatory response to NPP 4.*[335]

This Chapter provides more detail in regard to the data collected for analysis and the process of collection used to support this research.

## 4.2 METHODOLOGY

Part 2 of this research contains the detailed analysis of the oversight functions that are available to the Commissioner and the way that those functions have been exercised in regard to NPP 4. This analysis involved consideration of data gathered from various sources including annual reports; guidance, fact sheets and guidelines; audit reports; speeches; media releases and other public statements issued by the Commissioner and the OAIC. Detailed consideration has also been given to the case notes and OMI reports published by the OAIC and its predecessor, the OPC, to the extent they represent guidance issued by the Commissioner.

The same approach is used in the analysis of the Commissioner's exercise of its investigation powers, which is included in Part 3 of this research. This analysis focuses on the process used in the conduct of investigations and the reports issued by the Commissioner at the conclusion of investigations.

To support the analysis of the Commissioner's use of the investigations powers, 6 investigations, all of which related to NPP 4, are selected for more detailed consideration. Reports based on these investigations were published between February 2011 and July 2012. The 6 investigations considered in detail are:

1. *Vodafone Hutchinson Australia Own Motion investigation* (February 2011)[336] ('Vodafone OMI');
2. *Telstra Corporation Limited Own Motion Investigation* (July 2011) ('Telstra Mail Out OMI');[337]

---

335 See Chapter1.

336 Office of the Australian Information Commissioner, *Vodafone Hutchinson Australia Own Motion Investigation* (16 February 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/vodafone-hutchison-australia> ('*Vodafone OMI Report*').

3. *Sony PlayStation Network/Qriocity Own Motion Investigation* (September 2011) ('Sony OMI');[338]

4. *Telstra Corporation Limited: Own Motion Investigation* (July 2012) ('Telstra Bundles OMI');[339]

5. *Dell Australia and Epsilon: Own Motion Investigation* (June 2012) ('Dell/Epsilon OMI');[340] and

6. *Medvet Science Pty Ltd Own Motion Investigation* (July 2012) ('Medvet OMI')[341].

These 6 investigations were part of a series of 8 investigations, reports on which were issued by Timothy Pilgrim as Privacy Commissioner between February 2011 and April 2013, and all of which investigations included consideration of potential breaches of NPP 4 (or IPP 4, the equivalent applying to Commonwealth agencies).[342] The 6 cases selected are representative of the 8 investigations completed

---

337 Office of the Australian Information Commissioner, *Telstra Corporation Limited Own Motion Investigation* (7 July 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited-telstra> ('*Telstra Mail Out OMI Report'*).

338 Office of the Australian Information Commissioner, *Sony PlayStation Network/Qriocity Own Motion Investigation* (29 September 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity> ('*Sony OMI Report'*).

339 Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own Motion Investigation* (July 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited > ('*Telstra Bundles OMI Report*').

340 Office of the Australian Information Commissioner, *Dell Australia and Epsilon: Own Motion Investigation* (June 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/dell-australia-and-epsilon> ('*Dell/Epsilon OMI Report*').

341 Office of the Australian Information Commissioner, *Medvet Science Pty Ltd Own Motion Investigation* (July 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/medvet-science-pty-ltd-own-motion-investigation-report>('*Medvet OMI Report'*).

342 A list of all of the OMI Reports that have considered NPP 4 is included in Appendix B. Reports from OMIs conducted by the OAIC are published online. See Office of the Australian Information Commissioner, *Commissioner Initiated Investigation Reports* (30 June 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

during that time. They involve a range of different private sector respondents, different types of security incidents and different findings regarding breach of NPP 4. The 2 OMI Reports not considered as part of this research were excluded on the following basis:

- *Professional Services Review Agency: Own Motion Investigation* (December 2011):[343] This investigation involves the review of a government agency and consideration of IPP 4, rather than NPP 4. As referred to in Chapter 1.4, consideration of public entities' obligations pursuant to IPP 4 is outside the scope of this research;
- *First State Super Trustee Corporation: Own Motion Investigation* (June 2012).[344] This investigation related to a superannuation fund member reporting a web application error. The case turned more on the question of whether or not there had been a disclosure (given that it was a member of the fund who had identified the issue and accessed other members' personal information), rather than issues relating to NPP 4.

Data considered relevant to these investigations included the published OMI reports, media releases and statements issued by the OAIC together with information from the OAIC's investigation files accessed pursuant to two *Freedom of Information Act 1982*(Cth) requests, both of which are discussed further in the next section.

Since April 2013, the Commissioner has issued further reports on completed investigations regarding NPP 4.[345] These reports have not been considered in this research because they were issued after the researcher had submitted the request for access to records pursuant to the *Freedom of Information Act*.

---

343 Office of the Australian Information Commissioner, *Professional Service Revew Agency: Own Motion Investigation* (15 December 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/professional-services-review-agency>.

344 Office of the Australian Information Commissioner, *First State Super Trustee Corporation: Own Motion Investigation* <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/first-state-super-trustee-corporation-own-motion-investigation-report> ('*First State Super OMI Report*').

345 See Appendix B for a full list of OMI reports published by the OAIC, current as at July 2014.

## 4.3 DATA COLLECTION

Data was gathered from a number of different relevant primary and secondary sources. Primary sources included case law and legislative material including legislation, draft bills and explanatory memoranda. Secondary sources included journal articles; books; Parliamentary Committee reports and evidence given to Parliamentary Committees; Law Reform Commission discussion papers, issue papers and reports; newspaper articles and press and media releases. The main source of relevant data was the OAIC's own publications and material published on the OAIC's website including case notes and OMI reports; determinations; guides, fact sheets and information sheets; annual reports; audit reports, media releases and statements and reported speeches made by the Commissioner.

Additional data to support the detailed analysis of the 6 investigations was obtained from:

- Interviews conducted by the researcher with the Privacy Commissioner and the Acting Commissioner Compliance in December 2012; and
- Documents produced in response to requests to access records held by the OAIC made pursuant to the *Freedom of Information Act 1982* (Cth).

### 4.3.1 Interviews

It was initially anticipated that the researcher would conduct a series of interviews with the OAIC investigators responsible for conducting each of the 6 investigations. It was hoped that these interviews would provide detailed information about each investigation, including the reasons for undertaking the investigation, the steps taken in each investigation and the process used in coming to the conclusion reached in each case. Following approaches to the OAIC, it was agreed that Timothy Pilgrim, the Privacy Commissioner, and Angelene Falk, the then Acting Assistant Commissioner Compliance (ACC) would each make themselves available for a one hour interview with the researcher. These interviews took place on 14 December 2012 at the OAIC's Sydney premises.

The interviews took the form of semi-structured conversations, based on an interview guide which had been provided in advance to the interviewees.[346] This guide was used to help direct the interview to the key themes, which included:

- The skills and background of the OAIC personnel responsible for the investigations;
- The reason for undertaking the investigation;
- The planning for the undertaking of the investigations;
- The way that the investigations were conducted;
- The making of the decision in each case as to whether there had been a breach of NPP 4 and the standard used to determine that issue; and
- The process of reporting on the investigations and the publication of the reports.

Each interview was recorded and transcribed. A copy of the transcribed interview record was provided to each of the interview subjects, both of whom confirmed the accuracy of the transcript.[347]

Given the limited time available with the two interviewees, there was little opportunity to discuss in detail any of the individual investigations. The Acting Commissioner Compliance had also only recently taken that position, and so had not had an opportunity to familiarise herself with the details of the 6 cases selected for detailed consideration as part of this research. In view of these limitations, it was decided to submit a request for access to the OAIC's investigation files to allow the researcher access to more detailed information about how the investigations had been conducted.

---

346 A copy of the interview guide is included as Annexure F.

347 Email from Timothy Pilgrim to Jodie Siganto, 26 February 2013; Email from Angelene Falk to Jodie Siganto, 18 April 2013.

### 4.3.2 FOI Application

An application was made to the Privacy Commissioner pursuant to the *Freedom of Information Act 1982* (Cth) (FOI Act) for disclosure of all records relating to the Telstra incident investigated in 2011 (the Telstra Mail Out incident) on 8 September 2011. A response was received by email on 7 November 2011[348] identifying 10 documents as coming within the terms of the request. Nine out of the 10 documents were largely made available.[349] Only 1 document was redacted in full, on the basis that there would be so many deletions that producing the redacted document would 'provide no meaningful information' about the investigation.[350]

After first requesting administrative access,[351] which was refused,[352] a formal freedom of information (FOI) application covering the other 5 investigations was submitted to the OAIC on 21 May 2013.[353] The request was in the same terms as the previous FOI request and the request for administrative access. Following various extensions, a decision on the request was received on 30 August 2013.[354] A total of 220 documents were listed in the schedules attached to that document. Each investigation comprised between 26 and 40 documents, other than the Telstra Bundles case, which accounted for 82 documents. This was due in part to the greater number of file notes and to the number of emails individually disclosed that formed part of longer email chains.[355]

---

348 Letter from Mark Hummerston, Assistant Commissioner, Compliance OAIC to Jodie Siganto, November 2013 (OAIC Decision Letter PF49)

349 Some material was redacted pursuant to s 45C and s 47F of the FOI Act.

350 Letter from Mark Hummerston, above n 348.

351 Email from Jodie Siganto to Timothy Pilgrim, 21 March 2013.

352 Email from Angelene Falk to Jodie Siganto, 18 April 2013.

353 Email from Jodie Siganto to OAIC, 21 May 2013. A copy of the FOI Request is included in Appendix L.

354 Letter from Caren Whip to Jean Siganto, 30 August 2013.

355 For example, 30 individual files notes recording activity such as 'Sent close letter to NR for checking' were recorded in regard to the Telstra investigation. No other file had the same number of file notes.

An initial review of the documents received revealed that records relating to the interactions with Epsilon as part of the Dell/Epsilon investigation may have been overlooked. In response to a query in this regard, a further four documents were produced by the OAIC on 11 September 2013.[356] Following a more detailed review of the documents, there appeared to be further records that had not been disclosed. These missing records were identified, for example, from references made in other letters or emails and by reference to the documents listed in the case summary reports produced from the OAIC's case management system (called the 'Resolve "Actions" Report Print Out'). A list was prepared and sent by email to the OAIC, with a request for confirmation that these records were not held by the OAIC.[357] Subsequently, the OAIC confirmed that it had located an additional 51 records that had been overlooked as part of the initial search.[358] Administrative access (which had initially been denied when first raised in March 2013) was given to 19 of these 51 documents on 26 November, 2013.[359]

Further discussions then took place regarding how the remaining 32 documents were to be made available, with the OAIC advising that the failure to produce the documents subsequently located was deemed to be a decision to refuse to give access to the relevant records, dated the same date as that original disclosure.[360] After some consideration and consultation with the OAIC, the researcher agreed to make a new FOI request for access to the outstanding documents in early February 2014. As at 31 March 2014 those documents had not been made available and accordingly have not been considered as part of this research.[361]

---

356 Email from Caren Whip to Jean Siganto, 11 September 2013.

357 Email from Jean Siganto to Caren Whip, 28 October, 2013 , (Subject Header: Outcome of your Freedom of Information Request [DLM=Sensitive:Legal]).

358 Email from Caren Whip to Jean Siganto, 13 November 2013, (Subject Header: Your Freedom of Information Request, ref:# FOIREQ13 [DLM=Sensitive:Legal]).

359 Email from Caren Whip to Jean Siganto, 26 November 2013 {Subject header: Your Freedom of Information Request, ref:# FOIREQ13 [DLM=Sensitive:Legal]).

360 *FOI Act*, s 15AC.

361 A number of these documents were subsequently made available in late April 2014

Approximately 165 of the original 220 documents produced in response to the second FOI request made in May 2013 were redacted in whole or in part. The *FOI Act* provides that a number of exemptions are conditional, including the exemptions pursuant to sections 47C (deliberative process), 47E(d) (would have a substantial adverse effect on the operations of the agency) and 47G (would unreasonably affect the organisation in respect of its lawful business, commercial or financial affairs or prejudice the future supply of information to the agency). However, the Act also provides that these provisions should not prevent access to the records unless, on balance, access would be contrary to the public interest.[362] When considering the balance between these conditional exemptions and the public interest in non-disclosure, the decision-maker in the second case determined that:

- Providing access to the material deemed to be exempt pursuant to Section 47E(d) and 47G would materially adversely affect the willingness of organisations being investigated to cooperate with and provide information to the OAIC, upon which the OAIC is reliant; and
- The published OMI Reports already provided transparency of the OAIC's decision-making so that the public interest in scrutiny of the OAIC's decision-making was not given much weight.[363]

This reasoning, to the extent that it demonstrates the OAIC's concern to ensure the continued voluntary cooperation of respondents in OMIs, is relevant to the consideration of the use of the Commissioner's investigation powers in Part 3 of this research. The OAIC's view that the OMI reports are intended to provide transparency of decision-making, which is supported by the OAIC's response to the FOI request, is relevant to the consideration of the extent to which the OMI reports in fact provide transparency of decision-making included in Chapter 9.

---

362 Ibid s 11.

363 The extent to which the OMI Reports included in the case study in this research provide transparency of decision making is considered further in Chapter 9.10.2.1

## 4.4 METHOD OF ANALYSIS

A data management software tool, NVivo, was used to support the analysis of the data. All data was entered into this program, including the:

- Transcripts of the interviews with the Commissioner and the Acting Commissioner Compliance; and
- All records obtained through the FOI process prior to 30 March 2014, including the OAIC's decision letters.

All of the data was reviewed and analysed, having regard to the conceptual framework identified for analysis, using a technique known as 'coding.' The analysis, or coding, was a multi-step process. As a first step, all records were categorised by the type of record, for example, annual reports, OAIC media releases, other media publications and OAIC guidance. All of the documents relating to the 6 investigations were then coded separately by reference to the particular investigation to which they related. These records included interview transcripts, FOI documents, OAIC media releases and statements, other media reports and the published OMI reports. These records were then further coded by reference to the part of the investigation process that they related to, for example, initiation of investigation, request for information letters, responses from respondents and close letter. This analysis supported a better understanding of how each investigation had progressed and allowed for a comparison of each stage between the different cases. It supported, for example, the comparison of the terms of the different request for information letters that is included in Chapter 9.6.

The investigation records were then further coded by reference to concepts that related to the conceptual framework used in this research. As an example, the OMI Reports were coded based on the statements of principle made in regard to the Commissioner's interpretation of NPP 4, the security measures that should be in place, references to risk or contextual factors, and references to standards or guidance provided by the Commissioner. This coding supported an analysis of the extent to which the investigations could be said to be consistent with industry practice. The OMI reports were also coded based on the findings in regard to the security measures that were or were not in place, the findings of material facts and the reasons for the decisions. This coding supported an analysis of the extent to

which the investigations were consistent with the principles of procedural fairness and good decision-making, which principles in turn form part of the 'transparent, balanced and vigorous" framework used to assess the exercise of the Commissioner's powers. Based on this initial analysis, some themes began to develop, such as the 'on the papers' investigation process used, limited but conciliatory interaction with respondents and the time taken to complete each stage of the investigation.

These findings were then compared to the initial coding results from the analysis of the interviews, and all of the other data including speeches, media releases, annual reports and audit reports. From these some further themes started to develop, such as interaction with the media, reference to guidance, resource constraints and an interest in reaching agreement with the respondent on the outcomes and ability to report publicly that any issues had been addressed. These codes were then associated with different categories that were further refined by iterative analysis and coding of all of the data, until 3 main categories were derived: the OAIC's powers and its view on the use of those powers, the investigation process and the different steps within that process, and the Commissioner's interpretation of 'reasonable steps' for the purposes of NPP 4. Each of the identified themes could be aligned with one of these categories, and the 3 categories themselves directly related to the two conceptual frameworks used for the analysis. An outline of this category model and the themes within each is included in Appendix H. This model was used to shape the narrative of the findings contained in Chapters 5, 6, 9 and 10.

## 4.5 CONCLUSION

In this chapter, the data collected for analysis to assist in answering the questions posed by this research and the method used to analyse that data have been discussed.

For the analysis of the Commissioner's use of its oversight powers, data from a wide range of largely publicly available sources was collected and considered. By contrast, the enquiry into the Commissioner's use of its investigation powers uses data obtained substantially as a result of the researcher's request to access the OAIC's investigations records pursuant to the *Freedom of Information Act 1982* (Cth). The data requested related to 6 recent investigations selected for detailed

consideration. These 6 investigations were selected from the 8 investigations that were reported on between February 2011 and March 2013.

Information obtained from interviews conducted with the Privacy Commissioner and the Assistant Commissioner Compliance was also used to support the analysis of the use of the Commissioner's oversight and investigation powers.

All data was analysed with the assistance of a data management software tool. This tool helped identify themes relevant to the conceptual framework to be used for the analysis of the data. This conceptual framework is based on two lenses as developed in Chapters 2 and 3: consistency with an industry standard approach to information security; and the extent to which the exercise of powers could be regarded as transparent, balanced and vigorous. The results of the analysis of the data using this conceptual framework are contained in Parts 2 and 3 of this research. Part 2 will consider the use of the Commissioner's oversight powers, including the power to monitor, advise, educate and provide guidance, while Part 3 will consider the use of the Commissioner's investigation powers. The final consideration of the answer to the research question raised by this research and general conclusions are included in Chapter 11.

# PART 2: OVERSIGHT POWERS

# Chapter 5: Monitoring, Audit, Advice and Education

## 5.1 INTRODUCTION

This Part 2 examines the Commissioner's use of its oversight powers to monitor, audit, advise, educate and provide guidance to the community in regard to NPP 4.

Echoing Julia Black's analysis of the importance of monitoring, advice, education and guidance as indicators of an effective principle-based regulatory system,[364] the ALRC referred to the oversight powers as being necessary for a 'consistent dialogue between the regulator and regulated to [develop] a shared understanding of the objectives.'[365] The ALRC believed that the Commissioner's use of its oversight functions would enable them to be proactive in increasing people's awareness and understanding of privacy in order to prevent non-compliance, which was a critical role in the ALRC's recommended regulatory model for privacy. According to the ALRC, it was important that these functions be interpreted broadly, and resourced effectively.[366]

Consistent with a responsive regulatory approach, the OAIC itself has long articulated a preference for the use of its oversight powers over its more punitive enforcement powers:

> The Office's emphasis will be on providing advice, assistance and information. This is our first and preferred approach at all times. Our

---

[364] Black, above n 179, 439. See also the discussion in Chapter 2.5.

[365] *For your information,* above n 32, [4.68].

[366] Ibid [47.19].

> experience indicates that such an approach will be all that is necessary to resolve the large majority of matters that come to our attention.[367]

The Commissioner's preference for the use of the oversight powers has also been noted in the literature.[368]

The Commissioner's oversight powers pursuant to the *Privacy Act* included:

- Monitoring and research – including undertaking research into and monitoring developments in data processing and computer technology to ensure that any adverse privacy effects of such developments were minimised, monitoring and reporting on 'the adequacy of equipment and user safeguards,'[369] conducting agency audits,[370] and examining proposed enactments for potential privacy impact;[371]
- Advice – including advising and reporting to a Minister 'on any matter relevant to the operation' of the *Privacy Act*[372] and informing the Minister of action needed to be taken by any government agency to achieve compliance with the Information Privacy Principles;[373] and
- Education – for the purposes of promoting the protection of individual privacy, to undertake educational programs on the Commissioner's own behalf or in co-operation with other persons or authorities acting on behalf of the Commissioner;[374] and

---

367 *Information Sheet 13*, above n 203. The use of the term "at all times" could indicate that the Commissioner's preference for the use of guidance and education powers may in fact exceed that recommended by Ayres and Braithwaite in their pyramid of regulatory responses.

368 See, eg, Tim Dixon (ed), *Australian privacy reporter: a guide to privacy law and practice* (, [3-450].

369 *Privacy Act* s 27(1)(q) (previous provision).

370 Ibid s 27(1)(h) and (ha) (previous provision).

371 Ibid s 27(1)(b) (previous provision).

372 Ibid s 27(1)(f) (previous provision).

373 Ibid s 27(1)(j) (previous provision).

374 Ibid s 27(1)(m) (previous provision).

- Guidance – including publishing binding guidelines and non-binding fact sheets, information sheets and guidelines.[375]

Chapter 5 examines the use of the monitoring, audit, advice and education powers. In view of the importance of the guidance power to both principle-based regulatory systems and the responsive regulatory approach, the use of this power is considered separately in Chapter 6. The question of how appropriately each of these oversight powers has been exercised in regard to NPP 4 will be considered through the dual lens of consistency with an industry standard approach to information security; and the extent to which the exercise of powers could be regarded as transparent, balanced and vigorous.

## 5.2 MONITORING

### 5.2.1 Monitoring and Research Power

In the *Privacy Act*, the Commissioner's monitoring power is included as part of the research function. In addition to monitoring developments in data processing and computer technology, there is also a power to 'monitor and report on the adequacy of equipment and user safeguards.'[376]

In its review of the monitoring and research function, the ALRC recommended that, given the serious impact technology can have on privacy, the Commissioner's research and monitoring function should be extended to cover all relevant technologies, and not just computer technology.[377] The ALRC saw research and reports to the Minister as 'an excellent medium to guide policy in these areas and to increase awareness of the issues raised by particular technologies.'[378] This

---

375 Ibid s 27 (1) (e), 'to prepare and publish in such manner as the Commissioner considers appropriate, guidelines for the avoidance of acts or practices ... that may ... be interferences with the privacy of individuals ...' (previous provision). This is in addition to the power to issue guidelines relating to approved privacy codes, and under the *Data Matching Program (Assistance and Tax) Act 1990* and section 135AA of *the National Health Act, 1953*.

376 Ibid. The new provision is contained s 28A(2)(f).

377 *For your information,* above n 32, [47.20].

378 Ibid [47.21].

recommendation was accepted and the amended provision now refers to monitoring development in 'data processing and technology.'[379]

Monitoring for compliance is an important part of the compliance-based enforcement approach. Within a compliance-focused regulatory regime, monitoring recognises that agencies and organisations can decide the steps they will take to achieve the outcome set by the principle, and provides an avenue for the regulator to assess whether those steps are adequate in an educational, non-confrontational and facilitative manner. 'Monitoring determines whether the system is achieving its aims.'[380] The ALRC noted the importance of the use of the oversight powers to provide a constant update on compliance levels, as well as intelligence into how compliance programs were working.[381] However, the *Privacy Act* does not expressly confer power on the Commissioner to monitor compliance with the Act. This means that the Commissioner's express monitoring functions as provided in the Act are more limited than the 'informed monitoring for non-compliance' function referred to by Parker[382] and noted by the ALRC as an important proactive tool to secure compliance.[383]

### 5.2.2 Use of Monitoring Power

The *2013 OAIC Annual Report* refers to the range of activities carried out by the OAIC, including monitoring statutory compliance.[384] However, no more specific information is provided as to what those monitoring activities might comprise.

---

379 *Privacy Act*, s 28A(2)(D).

380 C Parker, 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 29, 35, quoted in *For your information,* above n 32, 238.

381 Ibid.

382 Ibid.

383 *For your information,* above n 32, [4.69].

384 Office of the Australian Information Commissioner, 'Annual Report 2012 - 2013' (2013) <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf>, 10 ('*OAIC 2013 Annual Report'*).

Monitoring, other than monitoring of data matching activities, is not referred to.[385] Its annual report from the previous year also referred to 'sustained attention' being given to each of the OAIC's roles, which included monitoring compliance with privacy laws.[386] However, that report also fails to provide any specific reference as to what those monitoring activities might have comprised. Similarly, there are no references in either report to monitoring of 'the adequacy of equipment and user safeguards' (in accordance with previous Section 27(q), of information security requirements or practices, or of compliance with NPP 4 more generally.

An internet privacy sweep carried out by the Commissioner as part of an international initiative by members of the Global Privacy Enforcement Network may be regarded as an example of proactive compliance monitoring.[387] The OAIC examined 47 websites that it believed were the most used by Australians in order to assess each site's privacy policy for accessibility, readability and content as well as its transparency.[388] The anonymised results were reported via media release.[389] It is not clear whether the Commissioner discussed the results of the sweep directly with the entities involved or took any other action to ensure remediation of identified issue, other than publication of the general findings by press release. The OAIC did issue a statement confirming that it would use the findings to inform the development of guidance about privacy policies.[390] In May 2014, a new guide was released to help entities prepare and maintain a privacy policy, although this guide makes no specific

---

385 The *Data-matching Act* provides that the Australian Information Commissioner is responsible for monitoring the functioning of the statutory data-matching program. The OAIC discharges this function by running data-matching inspections. See *OAIC 2013 Annual Report*, above n 381, 80.

386 *OAIC 2012 Annual Report*, above n 1, 4.

387 Office of the Australian Information Commissioner, 'Privacy Commissioner: Website privacy policies are too long and complex' ( Media Release, 14 August 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex>.

388 *OAIC 2013 Annual Report*, above n 381, 30.

389 Office of the Information Commissioner, above n 387.

390 Ibid.

reference to any findings from the earlier policy sweep.[391] There is no evidence of any similar activity being taken in regard to compliance with NPP 4.

In the context of NPP 4 and the ALRC's exhortation that the oversight powers should be interpreted broadly, the specific power to monitor the adequacy of equipment and user safeguards might be regarded as authorising a more proactive role in relation to new technology and business processes and any accompanying security issues. However, there is little indication that the OAIC has used its monitoring function in a proactive manner to either check compliance with NPP 4 or provide advice generally on security issues raised by new technology.

### 5.2.3 Analysis

The absence of evidence of any use by the OAIC of its monitoring power, whether generally in regard to compliance or more particularly in regard to compliance with NPP 4, has important consequences for the operation of the responsive regulatory approach. As discussed, monitoring of compliance is essential to the success of that approach.[392]

Conducting audits is another method for checking compliance. Use of the audit power has been referred to as the most visible sign of the Commissioner's use of its general monitoring powers and, according to the ALRC, is 'one of the few proactive regulatory tools' vested in the Commissioner.[393]

## 5.3 AUDIT

### 5.3.1 Audit Power

The Commissioner has various audit powers. For the purposes of this research, the most relevant is the power to audit the compliance of public entities, that is Australian and ACT government agencies, with the Information Privacy

---

391 Office of the Australian Information Commissioner, 'Guide to developing an APP privacy policy' (May 2014) < http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy.

392 See the discussion in Chapter 5.2.1.

393 *For your information*, above n 32, [47-103].

Principles.[394] In addition, under the previous regime, the Commissioner may have audited private sector organisations covered by the Act if requested by them. However, there is no indication that this power has been used.[395]

As part of its 2008 review, the ALRC recommended that the Commissioner be empowered to conduct privacy performance assessments, referred to as PPAs, on the levels of compliance in organisations more generally.[396] This was accepted, and the audit power has been extended to apply to private entities well as public entities.[397] The word 'audit' has also been replaced by the term 'privacy performance assessment,' reflecting the ALRC comment that use of the term 'audit' may have inherent negative connotations. This new assessment function, however, is 'curiously located outside the "monitoring" functions, and without the benefit of the important "powers" clauses that currently apply.'[398] Further consideration of the amended provision is outside the scope of this research.

The ALRC noted that audits can be used to take a snapshot of the level of compliance in an agency or organisation or across an industry.'[399] It referred to the deterrent effect of audit powers noting that 'the presence of an audit power can act as an important preventative measure,' because 'the existence of the audit functions and programs encourages organisations subject to the Act to take compliance seriously.'[400] However, it also regarded audits as having an educative role, recommending the change of terminology from 'audit' to 'privacy performance assessment' to emphasise the 'educational and non-confrontational nature of the process.'[401] This is consistent with the view of the OAIC. The most recent annual

---

394 *Privacy Act* s 27(1)(h) (previous provision).

395 Ibid s 27(3) (previous provision). In a November 2013 speech, the Privacy Commissioner noted that private entities had not ' invited' him in, see Timothy Pilgrim, above n 201.

396 *For your information,* above n 32, [47.104].

397 *Privacy Act* s 33C.

398 Greenleaf and Waters, above n 64.

399 *For your information,* above n 32, [47-98]-[47-100].

400 Ibid.

401 *For your information,* above n 32, [47.104].

report describes the OAIC audits as 'an educative process' and notes that they 'have been the catalyst for improvements to agencies' data security, accuracy of information, staff training and disclosure policies.'[402]

It has also been suggested that audit findings provide another source of guidance regarding what the Commissioner considers to be "reasonable steps" to secure personal information.[403] Although consideration of compliance with IPP 4 is outside the scope of this research, these audits are still relevant to the extent they provide guidance as to the Commissioner's interpretation and application of IPP 4, which has some overlap with NPP 4 and in the absence of any power to audit compliance with NPP 4.

### 5.3.2 Use of Audit Powers

The audit power has been used by the Commissioner more frequently than the general monitoring power. The actual number of audits conducted each year has varied, 'depending on the nature of privacy complaints and other priorities of the Office.'[404] However, generally the numbers are low and seem to be declining.[405]

According to the Commissioner's annual reports, nine (9) audits were conducted in 2009 – 2010, which was a 'significant increase' over the previous year,[406] while only five audits were conducted in 2010 – 2011.[407] The *OAIC 2011 Annual Report* noted this decline and stated that the Compliance Branch was

---

402 *OAIC 2013 Annual Report,* above n 381, 86. See also Office of the Australian Information Commissioner, *Privacy Performance Assessment Manual* (2012) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/privacy-performance-assessment-manual> 'Purpose of a privacy performance assessment', ('*Privacy Perfomance Assessment Manual'*).

403 Interpreting the Security Principle, above n 57, 22 - 23.

404 Office of the Privacy Commissioner, *The Operation of the Privacy Act Annual Report: 1 July 2006–30 June 2007* (2007), 60, referred to in *For your information,* above n 32, [47.88].

405 See, eg, Interpreting the Security Principle, above n 57, 22 – 23, which notes that 'Resource constraints have meant a marked reduction in the number of audits conducted in recent years.'

406 Office of the Privacy Commissioner, *2009-10 Annual Report of the Office of the Privacy Commissioner* (2010) < http://www.oaic.gov.au/about-us/corporate-information/annual-reports/office-of-the-privacy-commissioner-annual-reports/200910-annual-report-of-the-office-of-the-privacy-commissioner> 45 ("*OPC 2010 Annual Report")* .

407 *OAIC 2011 Annual Report,* above n 1, 42.

focusing additional resources on high-profile OMIs 'which required more extensive information-gathering and analysis.'[408] Three audits were conducted in 2011 – 2012[409] while four audits were commenced and five were finalised in 2012 – 2013.[410]

Audit reports are published on the Commissioner's website.[411] From March 2004 to October 2010 the reports of thirteen (13) audits of federal and ACT government agencies conducted by the OPC were published.[412] After the OAIC took over that function in November 2010, its audit team has separately published a further fourteen (14) reports (as at July 2014).[413] This amounts to a total of 27 audit reports published over a ten- year period.

Summarised details of completed audits are also included in the OAIC's annual reports.[414]

The OAIC's audits tend to relate to complex systems' handling of sensitive information (such as the operation of the Healthcare Identifiers System).[415] This is consistent with the risk-based targeting approach to conducting audits, which is discussed further below. A number of systems have been audited multiple times. The Australian Customs and Border Protection Service's dealings with EU

---

408 Ibid.

409 *OAIC 2012 Annual Report*, above n 1, 48.

410 *OAIC 2013 Annual Report,* above n 381, 86.

411 See Office of the Australian Information Commissioner, 'Audit Report' (2 July 2014) < http://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/ >. A list of all the OPC and OAIC published audit reports is included in Appendix K.

412 Ibid.

413 Ibid.

414 See, eg, *OAIC 2013 Annual Report,* above n 381, 86 – 89; *OAIC 2011 Annual Report*, above n 1, 42 – 45.

415 Office of the Australian Information Commissioner, 'Healthcare Identifiers Service — Department of Human Services: Audit Report' (April 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/healthcare-identifiers-service-department-of-human-services>; Office of the Australian Information Commissioner, 'Healthcare Identifiers Service: Audit report' (June 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/healthcare-identifiers-service-audit-report>.

Passenger-Name Records have been audited on four different occasions,[416] while the Department of Foreign Affairs and Trade's National Document Verification System has been audited six times.[417]

The OAIC has published a *Privacy Performance Assessment Manual* that describes in detail the OAIC's approach to audits, or privacy performance assessments as they are now known.[418] As a first step in the assessment cycle, entities are identified for assessment by using risk, based on background research.[419] The *Manual* provides an example of the identification of two ACT government agencies to be assessed, pursuant to the OAIC's Memorandum of Understanding with the ACT government.[420] However, is not clear that this risk-based targeting method has been used in the identification of Commonwealth agencies for assessment. There is no reference to the use of targeting as the basis for the audit in any of the reports. In any case, as at June 2014, OAIC audits were still only undertaken where supported by a specific funding agreement or Memorandum of Understanding.[421] This was confirmed in the researcher's interview with the

---

416 Office of the Australian Information Commissioner, 'Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report' (June 2013); Office of the Australian Information Commissioner 'Passenger Name Records (PNR data) Australian Customs and Border Protection Service Audit Report' (July 2013); Office of the Privacy Commissioner, 'Passenger Name Records (PNR data) Audit Report No 1' (December 2009); Office of the Privacy Commissioner, 'Passenger Name Records (PNR data) Audit Report No 2' (January 2010). Further details of the reports are included in Appendix K.

417 Reports were issued in May 2007, June 2011 and December 2012, however Office of the Australian Information Commissioner, 'National Document Verification Service - Department of Foreign Affairs and Trade - Audit Report 2012' (December 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/national-document-verification-service-department-of-foreign-affairs-and-trade-audit-report-2012>, [1.18] refers to there being six (6) audits of the system. Further details of the reports are included in Appendix K.

418 *Privacy Performance Assessment Manual*, above n 402.

419 *Privacy Performance Assessment Manual*, above n 402, 'Risk Assessment.'

420 *Privacy Performance Assessment Manual*, above n 402, 'Stage one: Targeting.'

421 See, eg, Office of the Australian Information Commissioner, 'Requests for Information for Passenger-Name Records Data – Australian Customs and Border Protection Service Audit Report' (June 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/requests-for-information-for-passenger-name-record-data-australian-customs-and-border-protection-service-audit-report>, [1.1], which report refers to the Memorandum of Understanding between the Australian Customs and Border Protection Service and the OAIC to

Assistant Commissioner Compliance who also said that this limitation on the proactive use of the audit power was a consequence of resource issues.[422] The reliance on independent funding might indicate that assessments are not always carried out based on the risk assessment process referred to in the *Manual*.

According to the *Privacy Performance Assessment Manual*, once the assessment is approved, the scope of the assessment and its objective are determined.[423] IPP 4 (the federal agency equivalent of NPP 4) was specifically considered as part of the scope of all audits where reports were released up to June 2013.[424] However, IPP 4 was within the scope of only one of the five audits where reports were issued between June 2013 and June 2014.[425] It is not clear whether there is any reason for the more recent audits being more limited in scope than previous assessments.

The objective of most assessments is to establish how well an agency is complying with its IPP obligations in handling records containing personal information,[426] although compliance with any special agreements and an agency's own documented controls, policies and/or procedures may also be considered.[427] Once what is being assessed and the objectives of the assessment are established, these are then used to develop the assessment criteria.[428] It might be expected that the *Manual* would provide some detailed guidance regarding how those criteria may be defined. The *Manual* does refer to sources such as the *Plain English Guidelines*

---

provide a regular audit program for Custom and Borer Protection's use of European-Sourced Passenger Name Record data.

422 Interview with Acting Commissioner Compliance (Sydney, 14 December 2012).

423 *Privacy Performance Assessment Manual*, above n 402, 'Stage two: Planning'.

424 Details of whether or not IPP was included in the scope of each audit are included in Appendix K.

425 Details of whether or not IPP was included in the scope of each audit are included in Appendix K.

426 *Privacy Performance Assessment Manual*, above n 402, 'What is performance assessed against?"

427 *Privacy Performance Assessment Manual*, above n 402, 'What is performance assessed against?"

428 *Privacy Performance Assessment Manual*, above n 402, 'Developing assessment criteria.'

*to the Information Privacy Principles*[429] and *Privacy Impact Assessment Guidelines*.[430] The *Manual* also provides an example of criteria that may be used, where the assessment is to consider the agency's storage and security of records (covered by IPP 4). The suggested criteria applicable to that assessment included:

- Personal information held by the agency is protected against unauthorised access, use, modification or disclosure;
- Personal information held by the agency is protected against loss or misuse;
- The agency has adopted physical, technical and administrative safeguards to protect personal information;
- Security safeguards are appropriate given the sensitivity of the information; and
- Processes are in place to record access to electronic records and datasets containing personal information.[431]

These statements are a repetition of the wording of the principle itself, other than the reference to the adoption of physical, technical and administrative safeguards and some sort of access logging process. Although they are a reasonable high-level outline of what is required for compliance with IPP 4, it is difficult to characterise any of these statements as measurable criteria against which the adequacy of complex security controls should be assessed. There is also little reference to risk, other than the connection drawn between the sensitivity of the information and the appropriateness of the security safeguards in place.

In practice, the published reports suggest there is some common approach in the OAIC's auditing of compliance with IPP 4. Physical security and storage (or the

---

429 Office of the Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles* (October 1994) http://www.oaic.gov.au/images/documents/migrated/migrated/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_14.4.pdf.

430 *Privacy Performance Assessment Manual*, 'Developing assessment criteria.'

431 *Privacy Performance Assessment Manual*, 'Types of assessment criteria'

security of paper-based documents and physical facilities), [432] IT security (which extends to access controls and logging) and data retention issues are commonly considered.[433] However, there is no explanation regarding why these areas were selected for consideration and why, for example, application security, network security and personnel security were not.

Various recommendations regarding security controls that should be implemented are made in the audits, such as that the payload data transferred between systems should be encrypted[434] and that random audits of access to systems should be undertaken.[435] However, in most cases it is not clear what assessment criteria were used to arrive at these recommendations or to determine the adequacy of the controls which were in place.[436] In particular, there is no reference to the *Information Security Manual* which includes mandatory requirements and recommended approaches to security for federal government agencies.[437] Nor do any of the *Audit Reports* refer to compliance with any guidance issued by the

---

[432] *Privacy Performance Assessment Manual*, Footnote 9, which notes that these examples of general criteria relating to storage and security were drawn from the Office of the Information Commissioner (Queensland*) Privacy Self-Assessment Guide.*

[433] Office of the Australian Information Commissioner 'Public Transport Systems: MyWay audit' June 2013 < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/public-transport-systems-myway-audit#part3-issues>, [3.77] – [3.136].

[434] See Recommendation 3 'Department of Foreign Affairs and Trade, Department of Immigration and Multicultural Affairs and Centrelink: Document Verification Service Prototype', 3 and 19 - 20

[435] See, for example, Recommendation 2 'Australian Customs Service: SmartGate Automated Border Processing', 13.

[436] One exception to this is the consideration of the storage and security of EU-sourced Passenger Name Record (PNR) data, which was assessed by reference to security obligations in the data sharing agreement between the Australian government and the EU, Office of the Australian Information Commissioner, 'Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report' (June 2013) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/requests-for-information-for-passenger-name-record-data-australian-customs-and-border-protection-service-audit-report>

[437] The PSPF and the ISM were discussed in Chapter **3.4**.

OAIC.[438] The exception to this is the Passenger Name Records audits, which use contractual security requirements as the basis for the audit assessment.[439]

An example of the issues raised by the absence of specified measurable criteria or consideration of context in the assessment of security controls is provided by the audit of the MyWay public transport system.[440] The MyWay system operates like most transport stored-value card systems, where devices loaded on buses retain usage data in on-board systems. This data is downloaded and transferred to the main system via a wireless connection established between the on-board machine and wireless access points located at bus depots. Down loading occurs when the buses return to the depot each evening. The *MyWay Audit Report* notes this downloading practice, and refers to the wireless communication as a secure means of daily data transfer on the basis that there is no human access occurring during the transfer.[441] In the findings section it is noted 'with approval that MyWay appears to have robust measures in place to ensure the security of data in transit, including … the use of wireless transfers of information, instead of portable devices, which can get lost or misplaced.'[442] This finding seems to suggest that wireless transfer is inherently more secure than a more manual process. However, there is no consideration of either the authentication method used to access the wireless access points in the depots or the level of encryption used to protect the data that is transmitted. Without strong authentication restricting access to authorised users, wireless access points can be compromised and used as a beachhead to enable access to the entire corporate network.[443] Similarly, it is a reasonably trivial exercise to capture un-encrypted

---

438 The OAIC's guidance in relation to NPP 4 (which is also applicable to IPP 4) is considered further in the following Chapter.

439 Office of the Australian Information Commissioner 'Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report, [4.94] – [4.145].

440 Office of the Australian Information Commissioner, 'Public Transport Systems: MyWay audit' (June 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/public-transport-systems-myway-audit#part3-issues> ('*MyWay Audit*').

441 Ibid [3.135].

442 Ibid [3.149]

443 Wolfgang Osterhage, *Wireless Security* (Science Publishers, 1st ed, 2011), 58.

wireless transmissions or to de-crypt wireless transmissions that have relied on older encryption protocols such as WEP.[444] However, the report does not consider the security of the use of the wireless connection itself, either generally or in terms of the authentication method used or the level of encryption implemented to protect the data in transit. Accordingly, it is difficult to identify how it was determined that 'robust measures'[445] were in place to secure the wireless transfer of data.

The third phase of the assessment process is fieldwork, during which evidence is collected to assist in the determination of whether the assessment criteria have been met. This stage requires the OAIC assessor to answer two main questions: How much evidence is sufficient? Is the evidence valid and reliable?[446]

In deciding whether the evidence obtained is sufficient to rely on to make audit findings, the *Assessment Manual* directs the assessment team to consider both the volume of evidence and its completeness[447] Properties such as the source, nature (for example, documented versus verbal evidence) and authenticity of the assessment evidence needs to be considered when evaluating the reliability of the evidence. The *Manual* suggests that, in general terms, the reliability of the evidence gathered is greater where it is obtained directly by the auditors rather than from the agency being assessed. Evidence obtained from, or corroborated or certified by, independent sources outside an agency may be more reliable for the purposes of an assessment than that obtained solely from within the agency.[448]

It is not clear from the audit reports how systematic recent audits have been or the extent to which they involve independent verification of either the implementation or the operation of controls that the auditee advises are in place.

The more recent reports contain more detailed information about the methodology used to collect relevant evidence. For example, the *Passenger Name*

---

444 Ibid 62.

445 MyWay Audit, above n 440, [3.149].

446 *Privacy Performance Assessment Manual*, above n 402, 'Stage three: Fieldwork.'

447 Ibid.

448 *Privacy Performance Assessment Manual*, above n 402, 'Stage three: Fieldwork.'

*Record Audit Report* from June 2013 describes the methodology as semi-structured interviews with key staff, the inspection of records, the review of relevant material prepared by the organisation under audit to assist with the audit and a site inspection 'assessing physical and IT security and storage arrangements, including (but not limited to) relevant access controls, audit logs, and use of third party contractors if relevant.'[449] However, there is no reference to independent testing and important findings seem to be based on the information provided by the agency without independent verification. For example, the audit report states that Customs and Border Protection 'advised that backups of all PNR data are maintained on a separate tape, undertaken on a daily basis and stored securely.'[450] Backup procedures are an important security control and capable of being independently verified without great cost, for example by asking for the backup logs or to view the storage location. However, there is no evidence of this independent testing. Similar assertions are relied on in other reports.[451] Further examples are provided by the *MyWay Report*, which indicates reliance on statements about the login and password controls in place for the system being tested,[452] and on the auditee's intention to run three-monthly audits of the system to verify if any misuse had occurred;[453] and by the Canberra Institute of Technology (CIT) audit where reliance is placed on CIT's advice that

---

449 Office of the Australian Information Commissioner, 'Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report' (June 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/requests-for-information-for-passenger-name-record-data-australian-customs-and-border-protection-service-audit-report>, [2.10].

450 Office of the Australian Information Commissioner, 'Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report' (June 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/requests-for-information-for-passenger-name-record-data-australian-customs-and-border-protection-service-audit-report>, [4,135].

451 See, eg, Office of the Australian Information Commissioner, 'ACT Education and Training Directorate: Final audit report (Information Privacy Principles audit)' (December 2013) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/collection-and-requests-for-student-information>, [2.6] – [2.11]; Office of the Australian Information Commissioner 'National Document Verification Service, Centrelink - Audit Report' (June 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/national-document-verification-service-centrelink-audit-report>, [2.3] – [2.4], [3.2.1]-[3.2.22].

452 MyWay Audit Report, above n 440, [3.109].

453 Ibid [3.111].

access to different parts of the network (which stored personal information) was restricted.[454]

The reliance on evidence provided by the auditee without independent corroboration could be a consequence of the limited time allotted to conducting the audits. In most cases, the field work to support the audit findings is conducted over a one or two day period, which is short given the complexity of some of the systems being audited and the scope of the audits.[455]

### 5.3.3 Analysis

If, as part of its audits, the OAIC were using the industry practice approach to information security put forward by this research to determine compliance with IPP 4, the reports would refer to:

- The identification of the main risks to the security of the entity's information (or the assessment of those risks would be used to guide consideration of relevant aspects of the entity's security posture);
- The connection between those risks and the security controls in place, or which should be in place; and
- The governance processes around the operation of security controls.

However, the audit reports make no reference to risk or to any direct linkage between the specific circumstances of the different systems or processes being considered and the level of security.

There is no indication that a specific audit plan is developed for the different systems that are audited. As discussed, there is indication of the basis for the

---

454 Office of the Australian Information Commissioner, 'Collection and security of student personal information – Canberra Institute of Technology: Audit Report' (April 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/collection-and-security-of-student-personal-information-canberra-institute-of-technology-cit>.

455 See, eg, Office of the Australian Information Commissioner, 'Australian Federal Police (ACT Policing Branch) Audit Report' (July 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/australian-federal-police-act-policing-branch-audit-report>, [2.3]; Office of the Australian Information Commissioner 'National Document Verification Service, Centrelink - Audit Report' (June 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/national-document-verification-service-centrelink-audit-report>, [2.4].

selection of physical security and storage, IT security and data retention controls as the areas for consideration in each audit. In particular, there is no reference to the use of risk assessment to identify the specific controls that might be expected to be in place in the particular circumstances of the systems under assessment in each of the different audits. There is no reference to any other standard, such as the list of controls in ISO 27002 or the controls contained in the PSPF and the ISM, which might be used as the audit benchmark.

Similarly, there is no reference to how the auditor has assessed that the security measures which are in place are reasonable in each case. One of the consequences of the absence of any such objective standard for measuring the controls that are in place is that it is difficult to understand how it has been determined that the controls in place are appropriate in different circumstances. For example, it is not clear how it was determined in the MyWay audit that the use of wireless for the transfer of data is preferable to a manual process, or that the process of wireless transfer was using 'robust measures,' because there is no discussion of the basis for that assertion in the published report.

The educative value of the published audit reports suffers from the absence of reference to any process, standard or benchmark for the identification, selection or implementation of security controls, which makes it difficult to identify any general principles that could be used to support decisions regarding whether the security controls in place are adequate. The reports also could not be regarding as supporting an industry practice approach to security.

The publication by the OAIC of audit reports on its website and the inclusion of audit details in annual reports provides some transparency as to the exercise of those powers. However, there is less f transparency regarding the identification of the control areas for audit and the basis for the audit findings, as outlined in the above analysis.

In terms of the balanced use of the audit power, the following observations could be made:

- Out of the 18 different government departments and over 200 Commonwealth Government agencies required to comply with the provisions of the *Privacy Act*,[456] only 4 different Commonwealth agencies have been audited since 2010. Although this may be a consequence of the OAIC's risk based approach to selecting audit targets, a broader selection of agencies might have been expected;
- Since audits are undertaken only where funding arrangements are in place, they tend to relate to complex government systems. The reports could not be regarded as providing a snapshot of compliance across a broad range of different entities and systems;
- The reduction in the number of audits to enable the completion of OMIs means a greater focus on reactive rather than proactive actions. This in turn has implications for the balanced use of the Commissioner's powers. OMIs relate to breaches that have occurred and are essentially reactive, while audits are proactive undertakings that may prevent privacy breaches while also having general educative value; and
- The failure to consider compliance with IPP 4 as part of the scope in more recent audits may also affect the balanced use of the audit power.

In regard to the vigorous use of the audit power, the following observations could be made:

- The total number of 27 audits conducted is low and seems to be declining, apparently resulting from a shift of resources to OMIs. The number becomes even lower if based on the number of unique systems being audited. The 13 audits of Commonwealth Government agencies have considered only four different systems or processes, being the use of Health Care Identifiers, handling of Passenger Name Records, the

---

456 A list of Commonwealth government departments and agencies is published at < http://australia.gov.au/directories/australian-government-directories/list-of-departments-and-agencies>

Document Verification System and the new ePassport SmartGate system;[457]

- The length of time spent on site would suggest that little independent testing of large and complex systems is completed. This is further confirmed by reliance in the reports on information given by the entity under assessment without any independent verification. Considering these issues, it is difficult to regard the evidence relied on in the reports as complete, valid and reliable as contemplated by the *Privacy Performance Assessment Manual*.

Based on the above, although the published audit reports may be of some educative value, it is difficult to characterise the Commissioner's use of its audit power to date as transparent, balanced or vigorous. It is also difficult to see how these reports could act generally as the catalyst for improvements to agencies' data security, as asserted by the OAIC.

## 5.4 ADVICE

### 5.4.1 Advice Power

The Commissioner has several advisory functions under the *Privacy Act*. These include:

- Advising a minister, agency or organisation on any matter relevant to the operation of the *Privacy Act*;[458]
- Examining any proposed enactment that would require or authorise acts or practices which might be an interference with the privacy of individuals;[459] and
- Making reports and recommendations to the Minister in relation to any matter that concerns the need for, or the desirability of, legislative or administrative action in the interests of individuals' privacy.[460]

---

457 Details of all published audit reports are included in Appendix K.

458 *Privacy Act* s 27(1)(f) (previous provision). The new provision is s 28B(1)(a).

459 Ibid s 27(1)(k) ) (previous provision). The new provision is s 28B(1)(b).

Pursuant to these powers, the OAIC provides advice to:

- Commonwealth Government agencies;
- ACT Government agencies;
- The Norfolk Island Administration, from 1 January 2011;[461] and
- Businesses.[462]

The Commissioner's advisory functions were given limited attention as part of the ALRC review and no substantive recommendation was made for amendment.[463] However, the ALRC was of the view that advice (or a generalised form of it) should be made public where relevant to a broader audience and where it would increase understanding of the *Privacy Act*.[464]

### 5.4.2 Use of Advice Powers

The *OAIC 2011 Annual Report* was the first to provide details of the Commissioner's advice work.[465] Details about advice given and submissions made by the OAIC were also included in the *2012 Report*[466] and the *2013 Report*.[467] The *2013 Annual Report* lists advice provided to a large number of government agencies, cross-government consultative forums and other jurisdictions (such as the NT Information Commissioner and the Global Privacy Enforcement Network).[468] It also refers to advice given to private entities including a number of industry groups and

---

460 Ibid s 27(1)(r) (previous provision). The new provision is s 28B(1)(c).

461 *OAIC 2011 Annual Report,* above n 1, 25.

462 *OAIC 2013 Annual Report,* above n 381, 50 – 60; *OAIC 2012 Annual Report*, above n 1, 78 – 83; *OAIC 2011 Annual Report*, above n 1, 45- 48.

463 *For your information,* above n 32, [47.1]-[47.24]

464 Ibid [47.22].

465 *OAIC 2011 Annual Report*, above n 1 , 45 - 48.

466 *OAIC 2012 Annual Report*, 78 – 83.

467 *OAIC 2013 Annual Report,* above n 381, 50 – 60.

468 Ibid.

committees (such as the Communications Alliance and the Human Research Ethics Committee) and to Google and Facebook.[469]

Little detailed information is provided in regard to the actual advice given, particularly in regard to advice given to the private sector. For example, where describing advice given to the Communications Alliance on the monitoring of voice communications, the *2103 Annual Report* notes that the OAIC provided general comments on existing guidelines, which it regarded as providing a useful and detailed approach for relevant entities, and advised that the guidelines would need to be reviewed with the introduction of the APPs.[470] Similarly, the description of the advice provided to a Human Research Ethics Committee about the collection, use and disclosure of health information for research purposes states that advice was given in relation to research involving data linkage using health information and other personal information, including de-identified information. No detail is provided as to what that advice may have comprised.[471] By contrast, reference is made to advice given to the ACT Justice and Community Safety Directorate on their review of the *Workplace Privacy Act 2011*, which included that key privacy matters were absent from that Act, and describing some of those (such as the absence of a complaint process).[472]

Based on statistics released for 2014, the total number of submissions and policy advice provided by the OAIC has declined.[473] A comparison over the last three years is provided in *Table 2* below.

| OAIC Activity | 2012 | 2013 | 2014 |
|---|---|---|---|
| **Privacy policy advice** | Not available | 142 | 103 |

469 Ibid 55 – 58.

470 Ibid 57 - 58.

471 Ibid 57.

472 Ibid 55.

473 Office of the Australian Information Commissioner 'OAIC Quarterly Statistics 2013-14 as at 30 June 2014' < http://www.oaic.gov.au/images/documents/about-us/corporate-information/Budget-and-statistics/OAIC_statistics_2013-14_as_at_30_June_2014.pdf>.

| | | | |
|---|---|---|---|
| **Privacy submissions** | Not available | 25 | 15 |
| **Media enquiries (for all OAIC)** | 285 | 314 | 307 |
| **Presentations and speeches (for all OAIC)** | 44 | 55 | 79 |

*Table 2: OAIC community engagement activities*

The OAIC's submissions are published on the OAIC's website[474] although this does not seem to be a complete record of all submissions (based on the information in the OAIC Quarterly Statistics).[475] Similarly, details of some but not all of the privacy advice work undertaken by the OAIC are included in the OAIC's Annual Reports.[476]

### 5.4.3 Analysis

The OAIC's own statistics suggest a steep decline in 2014 in every area of support and advice in comparison to the previous year.[477] This decline is unexpected given the introduction of the new amendments, which might have been anticipated to lead to increased requests for advice from the OAIC.

Although there is some transparency in regard to the advice provided via the information published on the OAIC's website and included in its annual reports, this

---

474 Office of the Australian Information Commissioner 'Privacy Submissions' (30 June 2014) < http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/>. There are 10 submissions on the website for the period from April to June 2014, while the recent statistics state that 15 submissions were made. See Office of the Australian Information Commissioner 'OAIC Quarterly Statistics 2013-14 as at 30 June 2014' < http://www.oaic.gov.au/images/documents/about-us/corporate-information/Budget-and-statistics/OAIC_statistics_2013-14_as_at_30_June_2014.pdf>.

475 For example, there are 10 submissions on the website for the period from April to June 2014, while the recent statistics state that 15 submissions were made. See Office of the Australian Information Commissioner 'OAIC Quarterly Statistics 2013-14 as at 30 June 2014' < http://www.oaic.gov.au/images/documents/about-us/corporate-information/Budget-and-statistics/OAIC_statistics_2013-14_as_at_30_June_2014.pdf>.

476 See, e.g. *OAIC 2013 Annual Report,* above n 381, Chapter 4.

477 Office of the Australian Information Commissioner 'OAIC Quarterly Statistics 2013-14 as at 30 June 2014' < http://www.oaic.gov.au/images/documents/about-us/corporate-information/Budget-and-statistics/OAIC_statistics_2013-14_as_at_30_June_2014.pdf>.

is not exhaustive and, where published, is summarised at so high a level as to be of little general value (for example, the description of the advice provided to Human Research Ethics Committee discussed above). This is notwithstanding the ALRC's recommendation that advice be made publicly available, particularly where it is of general interest.[478] Accordingly, it is difficult to characterise the Commissioner's use of the advice power as either fully transparent or vigorous.

From the information that is available, it appears that the advice provided and the submissions made are largely reactive, that is, given in response to requests made for advice or for submissions. Other than the engagement with Facebook and Google, there is little indication of the proactive provision of any advice to the private sector. This suggests that the power is not used in a balanced manner.

Finally, none of this advice work referred to appears to have involved any significant general public advice in regard to NPP 4. This suggests again that the Commissioner may not be using its advice power in a vigorous or balanced way.

## 5.5 EDUCATION

### 5.5.1 Education Power

The Commissioner's oversight functions in relation to education include:

- Promoting an understanding and acceptance of the NPPs;[479] and
- Undertaking educational programs on the Commissioner's own behalf or in cooperation with others to promote the protection of individual privacy.[480]

This explicit role is in addition to the use of other powers, such as the audit power and the guidance powers, which are also intended to have an educative effect. The Commissioner's use of its guidance powers, including the issuing of non-binding guidance and the release of case notes and OMI reports, is considered separately in the next chapter.

---

478 *For your information,* above n 32, [47.22].

479 *Privacy Act* s 27(1)(d) (previous provision).

480 Ibid 27(1)(b) (previous provision). The new provision is included as part of the guidance related function in s 28(1)(d).

In its review, the ALRC referred to the pivotal role education plays in a principles-based regime such as the *Privacy Act*.[481] While submissions to the ALRC's review supported education and the Commissioner's role in providing education, they referred to the apparent lack of priority given by the Commissioner to the education function and the need for more guidance from the OPC to encourage an understanding of, and compliance with, the privacy principles.[482] The report does not contain any analysis of the use of the education power by the Commissioner as at the time of issuing the report, nor does it make any specific recommendations in regard to the education power. In the amended Act, the Commissioner's education powers are included as part of the guidance-related functions, but otherwise they are largely unchanged.[483]

### 5.5.2 Use of Education Powers

Historically, the Commissioner's ability to engage in educational programs has been constrained by available resources.[484] In 2006, the government committed to provide additional funding to allow the Commissioner to provide a comprehensive education program to raise community awareness of privacy rights and obligations.[485] Perhaps as a consequence of this commitment, the ALRC subsequently referred to the information provided by the OAIC through its information hotline and its website as part of the exercise of the education power. Since then, the avenues for the OAIC to provide information and education have grown, and now include newsletters and social media, including YouTube,[486] Twitter[487] and Facebook[488] together with an electronic newsletter.[489]

---

481 *For your information,* above n 32, [47.23].

482 Ibid, [47.14] – [47.18].

483 *Privacy Act*, s 28(1)(c) - (d).

484 See, eg, *Getting in on the Act*, above n 155.

485 Ibid rec 26. The Senate Committee privacy inquiry made a similar recommendation: Parliament of Australia—Senate Legal and Constitutional References Committee, The Real Big Brother: Inquiry into the *Privacy Act* 1988 (2005), rec 19.

486 <http://www.youtube.com/user/OAICgov>.

487 'OAICgov' https://twitter.com/OAICgov.

The Commissioner's education activities are said to be covered in Chapter 4 of the 2012 and 2013 annual reports, which chapter is headed 'Communication and Engagement.'[490] However, the only reference to 'education' in Chapter 4 of the *2013 Annual Report* is in the context of the OAIC's 'education and information' campaign supporting an understanding of the *Privacy Act* amendments, which included a dedicated page on the OAIC website, short videos, posters, training materials, a public consultation process and 'regular engagement with stakeholders.'[491]

Based on the information included in the annual reports and the recent statistics, it would seem that the OAIC's focus is on providing general information, promoting awareness and engaging with the media, rather than on providing specific education directed at a particular privacy principle or the application of a principle to a current issue.

There is evidence of increased engagement by the OAIC with the media. The 2013 annual report refers to a 10% increase in media responses over the previous year, mostly attributable to legislative changes and high-profile data breaches and the associated reports released by the OAIC.[492] The Commissioner also participated in a large number of interviews,[493] the transcripts of some of which are published on the OAIC's website.[494] The OAIC itself published 20 media releases in 2012–13.[495] NPP 4 and organisational responsibility to ensure the security of personal information is an issue often referred to by the Commissioner as a significant issue in

---

488 https://www.facebook.com/OAICgov.

489 *OAIC 2013 Annual Report,* above n 381, 26.

490 Ibid; *OAIC 2012 Annual Report*, above n 1, 27.

491 *OAIC 2013 Annual Report,* above n 381, 26.

492 The changes included the passing of the *Privacy Amendment Act* and the introduction of the Privacy Amendment (Privacy Alerts) Bill 2013. *OAIC 2013 Annual Report,* above n 381, 28.

493 *OAIC 2013 Annual Report,* above n 381, 28.

494 Office of the Australian Information Commissioner 'Privacy Speeches' < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/>

495 *OAIC 2013 Annual Report,* above n 381, 28.

its speeches and interviews, albeit in a general way.[496] The OAIC participated in Cyber Security Awareness Week in 2013[497] and Stay Smart Online Week (as it was renamed) in 2014.[498] This activity is consistent with the view expressed by the Commissioner in 2012 that the OAIC needed to be able to 'provide advice to the community on issues relating to the use of the online environment.'[499] However, there are few indications of more directed educative initiatives relating specifically to either NPP 4 or IPP 4, other than in regard to promotion of the *Guide to Information Security*, including its release by the then-Attorney General as part of the launch event for Privacy Awareness Week 2013.[500]

The OAIC has been active in promoting data breach notification, which might be regarded as part of taking reasonable steps to protect data.[501] The OAIC has released a guide on voluntary notification of data breaches.[502] The Commissioner

---

496 See, e.g., Timothy Pilgrim 'Privacy law reform – Get in on the Act' Presentation at the iappANZ Privacy Awareness Week seminar, Brisbane, 1 May 2013.

497 Office of the Australian Information Commissioner, 'Take time to protect your privacy during Cyber Security Awareness Week' (Media Release, 20 May 2013) < http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/take-time-to-protect-your-privacy-during-cyber-security-awareness-week>.

498 Office of the Australian Information Commissioner, "Stay Smart Online", OAIC Homepage (3 June 2014) < http://www.oaic.gov.au/>.

499 Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing* (14 February, 2012), 41 – 43.

500 Timothy Pilgrim 'Privacy Awareness Week 2013 Privacy Commissioner's Update' Presentation to Privacy Awareness Week 2013 Business Breakfast, Sydney, 29 April 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-awareness-week-privacy-commissioner-s-update>.

501 See, eg, Timothy Pilgrim, 'Mapping data breach notification' (Presentation at iappANZ data breach panel discussion, Sydney, 6 May 2014 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/>, Timothy Pilgrim, 'Privacy and Transparency' (Presentation to the Privacy Awareness Week 'Up close and personal' business breakfast, 5 May 2014).

502 Office of the Australian Information Commissioner, 'Data breach notification – A Guide to Handling Personal Information Security Breaches', April 2011 < http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/data-breach-notification-a-guide-to-handling-personal-information-security-breaches>.

regularly refers to voluntary notification as a desirable practice[503] and encourages entities to go to the OAIC for advice when they have experienced a data breach.[504]

The OAIC regards its handling of data breaches as part of its function to promote an understanding and acceptance of the NPPs (and presumably NPP 4 in particular).[505] The OAIC's annual reports include information about voluntary notifications of data breaches, including limited anonymised details about reported incidents. However, no more than one sentence is used to describe each incident, and in largely generic terms. Examples include 'a system error occurred, allowing customers to access other customers' records'[506] and 'the hacking of databases containing customers' personal information.'[507] Given their brevity, there is little from those statements that could be regarded as educative for other entities. In addition, the advice provided in the annual reports in regard to how to respond to a data breach incident (including updating systems and advising customers) appears to be formulaic. The OAIC reported the same actions taken by entities in response to a data breach notification in each of the 2011, 2012 and 2013 annual reports, notwithstanding that a wide range of different types of incidents were reported as occurring in each of those years.[508]

Recently, the OAIC has released Statements outlining the action taken by the OAIC in response to publicised data breaches, for example the AFP data breach,[509]

---

503 See, eg, Timothy Pilgrim, 'Australians better protected with mandatory data breach notification' (Media Release, 28 May 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australians-better-protected-with-mandatory-data-breach-notification>.

504 Timothy Pilgrim, 'Mapping data breach notification', above n 501.

505 *Complaints Manual* above n 226,, "Our role in DBNs" which refers to data breach notification cases as falling under *Privacy Act* Section 27(d).

506 *OAIC 2011 Annual Report* above n 1, 38.

507 *OAIC 2013 Annual Report,* above n 381, 79,

508 *OAIC 2013 Annual Report,* above n 381, 79, *OAIC 2012 Annual Report* above n 1, 65; *OAIC 2011 Annual Report*, above n 1, 38.

509 Office of the Australian Information Commissioner, 'AFP data breach', (Statement, 28 August 2014) < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/afp-data-breach/>.

the ACCC data breach[510] and the eBay data breach.[511] Most of these Statements are short and simply confirm that the OAIC is seeking more information about the particular incident, without providing any more general advice to affected individuals. For example, the Statement released in relation to the recent highly publicised data breach affecting eBay Systems provided in its entirety:

> The Office of the Australian Information Commissioner (OAIC) received a voluntary data breach notification from eBay Inc. early on 22 May 2014. We are currently conducting enquiries into the data breach to inform whether the OAIC will need to open an investigation.[512]

The purpose of this and the other similar Statements released by the OAIC is not clear, other than perhaps to reassure the community that appropriate action is being taken. It is difficult to regard this or any of the other Statements as educative, whether in regard to the factors that led to the breach, the precautions that people who might be affected should consider or how the OAIC might deal with the situation.

Little more detailed information is provided about any of the DBN cases outside of the annual reports and the Commissioner's Statements. In particular, there are few reports of DBN-based investigations. According to the OAIC's report, there were 46 DBNs in the 2011 – 2012 year.[513] However, of the OMI reports released since 1 July 2011, only two of those investigations seem to relate to DBN cases.[514]

---

510 Office of the Australian Information Commissioner, 'ACCC data breach' (Statement, 11 April 2014) < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/accc-data-breach/accc-data-breach>.

511 Office of the Australian Information Commissioner, 'eBay data breach'(Statement, 22 May 2014) http://www.oaic.gov.au/news-and-events/statements/privacy-statements/ebay-data-breach/ebay-data-breach.

512 Office of the Australian Information Commissioner, above n 511. Reporting on the breach included See, eg, Fran Foo, "Warning after eBay passwords 'stolen'" The Australian (*online*), 23 May 2014 < e6frgakx-1226927542280>; Brid-Aine Parnell "eBay faces Multiple Probes into mega-breach" The Register (*online*), 23 May 2014 <http://www.theregister.co.uk/2014/05/23/ebay_security_breach_investigations/.

513 *OAIC 2012 Annual Report*, above n 1, 64.

514 The two investigations are the Dell/Epsilon Investigation and the Telstra Bundles investigation. Both of these investigations are considered in more detail in Part 3 of this research.

This may reflect the fact that few data breach notifications lead to investigations. In any case, the limited reporting on DBNs raises the question as to how the practice of entities reporting data breaches may result in the OAIC promoting a more general understanding and acceptance of the NPPs.

### 5.5.3 Analysis

In summary, it seems that although the Commissioner has significantly increased its general information and awareness activities, as well as its media engagement, there is little that could be regarded as directed educational activity undertaken in relation to NPP 4. Although the OAIC has promoted the benefits of DBN, it is not clear how that process has been of any educative benefit to the wider community. To the extent that information has been made available about data breach notification cases it is difficult to derive any principles of more general application. There is certainly no link between the Commissioner's approach to data breach cases and an industry practice approach to information security,

## 5.6 CONCLUSION

The Commissioner has a range of oversight functions that include the provision of monitoring, auditing, advice and education and guidance, all of which were identified in Chapter 2 as fundamental to the success of both principle-based regulation and a compliance-based enforcement approach. In this chapter, those powers (excluding the guidance power) have been considered through the lens of the two conceptual frameworks: a standard approach to information security practice and the extent to which the exercise of regulatory powers could be regarded as transparent, balanced and vigorous. The following summarises the findings made.

There is little evidence of the Commissioner's exercise of its monitoring, advice and education powers to support an industry approach to information security. Of all the powers available, the Commissioner's use of its audit powers has most directly involved consideration of reasonable security. However, the reports from those audits do not suggest that the Commissioner is following the industry standard approach to information security put forward in this research. There is no reference to risk (in the context of IPP 4), nor is there evidence of the use of any particular standard or benchmark to either guide the audit activity in terms of the controls that

should be reviewed or to support the determination as to whether or not the controls that were identified could be regarded as adequate.

Other than general statements about the importance of security (and data breach notification in particular), the Commissioner has provided little other advice or education on how to ensure that personal information is properly secured.

The availability of materials including audit reports, speeches, submissions, Statements and Media Releases on the OAIC's website provides transparency about the exercise by the Commissioner of some of its oversight powers. However, the extent to which these publications provide transparency regarding the Commissioner's interpretation and application of NPP 4 is questionable. In particular, it is difficult to regard the Commissioner's audit reports as truly educative in terms of the Commissioner's interpretation or application of IPP 4.

There is little indication of any proactive monitoring of either 'the adequacy of equipment and user safeguards' as was specifically referred to in Section 27(q), or more generally of compliance, which the ALRC regarded as a fundamental element of the compliance approach to enforcement.[515] It is also difficult to characterise the Commissioner's audits as balanced or vigorous given the low number, the narrow group of entities that have been audited and the reactive, rather than proactive, nature of the use of the power.

These matters could well be a consequence of resourcing issues, which may also be responsible for the limited time spent on site by the OAIC team and the reliance on information provided by the entity under audit rather than on the auditors' own independent findings. Resourcing issues may also be responsible for the decline in the number of audits, submissions and responses to requests for advice made by the OAIC. Although more information about the Commissioner's initiatives in these areas is available than has previously been released, that information is still high-level and not particularly educative.

Although efforts have been taken to educate the public about both the privacy reforms and the new *Guide to Information Security* (which is covered in more detail

[515] See discussion in Chapter 5.2.

in the next chapter), there is little evidence of any systematic or comprehensive education program in regard to NPP 4. The OAIC refers to its dealing with reported cases of data breach as being pursuant to its advice and education functions. However, although the Commissioner may provide useful advice and guidance as part of its direct engagement with the entity that has notified of the breach, it is not clear how the reporting of data breaches assists in a more generally educative way.

Based on the above, it could be said that oversight functions have not so far been exercised in an entirely transparent, vigorous or balanced way in regard to NPP 4 (although there have been some recent improvements generally in the OAIC's transparency and community engagement). There are also gaps between the exercise of these oversight functions and an industry practice approach to information security.

However, this chapter has considered only the Commissioner's monitoring, audit, advice and education powers. The Commissioner's oversight powers also include the power to provide guidance, which is perhaps the most important power given the nature of PBR. The Commissioner's exercise of its guidance powers is considered in the next chapter.

# Chapter 6: Guidance

## 6.1 INTRODUCTION

The Commissioner is required to make or approve a number of legally binding privacy guidelines although this power is limited to specific areas (such as health research[516]). The Commissioner has no power to issue legally binding guidelines in regard to NPP 4. However, the *Privacy Act* also confers wide powers on the Commissioner to issue non-binding guidance including the power to make 'guidelines for the avoidance of acts or practices … that may … be interferences with the privacy of individuals.'[517]

Guidance helps combat issues caused by the vagueness and lack of certainty as to the meaning of the privacy principles. Guidance together with education is also a key component of the base level of the Ayres and Braithwaite enforcement pyramid.[518] The ALRC referred to guidance as an essential requirement for the effective operation of the principle-based regime in the *Privacy Act*.[519]

A regulator can provide guidance in a number of forms, including education programs, audit reports and other uses of the Commissioner's oversight functions. These other types of guidance were considered in the previous chapter. This chapter will assess those documents issued pursuant to the Commissioner's express power to issue non-binding under the *Privacy Act*. These documents include non-binding guides, guidelines, fact sheets and resources.[520] These publications 'represent the

---

516 *Privacy Act* s 95.

517 Ibid s 27(1)(e) (previous provision). The new provision is s 28 (1)(a).

518 See the discussion in Chapter 2.5.

519 *For your information,* above n 32, [4-59].

520 These documents are published on the OAIC website at different pages. See, eg, Office of the Australian Information Commissioner 'Advisory Privacy Guidelines' < http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/> Office of the Australian Information Commissioner 'Privacy Fact Sheets' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/>.

public position of OAIC and should guide the application of the law to complaints' however they are not binding and should not be regarded as law.'[521] Consideration will also be given to published investigation reports, which can also be regarded as providing guidance.

The ALRC considered the Commissioner's powers to issue guidance to be sufficiently broad.[522] However it noted concerns with the Commissioner's record of issuing 'vague and ambiguous' guidelines and its failure to engage in a well-resourced and properly conducted consultation process as part of the development of previous guidelines.[523] A submission to the ALRC Inquiry by Professor Greenleaf and others contended that before issuing guidance 'the Commissioner should be required to consult with interested parties and to have regard to the differential resources and capacities of different groups of stakeholders.'[524] This submission was not accepted.

Details of the year and type of publication issued by the OAIC that could be regarded as guidance are included in the table below.[525]

| | 2014 | 2013 | 2012 | 2011 | 2005 - 2010 | 2001 - 2004 | Earlier & Undated | Total |
|---|---|---|---|---|---|---|---|---|
| **Guideline** | 2 | 2 | | | | | | **4** |
| **Guide** | 8 | 2 | | | 1 | 3 | 7 | **21** |
| **fact sheet** | 27 | 1 | 7 | 5 | 13 | 6 | 3 | **62** |

521 *Complaints Manual*, above n 227, 8.

522 *For your information,* above n 32, [47.35]: 'The Commissioner's function in s 27(1)(e), as currently drafted, is broad enough to enable the Commissioner to issue guidance on a range of matters, particularly when read in conjunction with the Commissioner's powers to provide advice, promote an understanding of the NPPs and IPPs, and undertake education programs. For these reasons, the ALRC is not recommending any reform to the guidance function.'

523 Ibid.

524 Waters, Greenleaf, Bygraves and Roth 'Promoting and Enforcing Privacy Principles', above n 65, 7.

525 A full list of these publications is included in Appendix M. This list is correct as at 30 September, 2014.

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| **Privacy Agency Resource** | 2 | 1 | | | | | 1 | **4** |
| **Privacy Business Resource** | 4 | 2 | | | 2 | 4 | 1 | **13** |
| **TOTAL** | **43** | **8** | **7** | **5** | **16** | **13** | **12** | **104** |

*Table 3: OAIC published guidance at 10 September, 2014*

With the amendments becoming effective in March 214, significant new guidance was published and old guidance has been removed.[526] The bulk of the new publications are fact sheets.[527] Of the 27 fact sheets issued in 2014, 23 were directed to two issues: 16 fact sheets dealt with issues relating to changes to the credit reports provisions and 7 related to dealing with e-health records. Guidance on the new APPs has also been issued.[528] This new guidance is similar to that published previously in regard to the NPPs which had been criticised as vague and high-level.[529] The preparation of this material has involved a considerable amount of work for the OAIC,[530] and will continue to do so as the Commissioner has indicated that further guidance is still to be issued.[531] The Commissioner has said the OAIC

---

526 For example, Privacy Fact Sheets 13, 14 and 16 are no longer published on the OAIC's website. See 'Privacy Fact Sheets' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/>. The *Complaints Manual* is also no longer published in the OAIC's website.

527 Facts Sheet and other guidance published by the OAIC and its predecessor the Office of the Privacy Commissioner are available online at Office of the Australian Information Commissioner 'Privacy Fact Sheets' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/>.

528 Office of the Australian Information Commissioner 'APP Guidelines' <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, ('*APP Guidelines'*).

529 Greenleaf, Bygraves and Roth 'Promoting and Enforcing Privacy Principles', above n 65, 7.

530 *OAIC 2013 Annual Report,* above n 381, xiv.

531 Timothy Pilgrim, Privacy Commissioner 'Privacy Reform – Act Three' (Presentation to the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013) < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>. See also Office of the Australian Information Commissioner, 'OAIC Privacy Law Reform Guidance Consultation and Publication Guide' (11 December 2013) < http://www.oaic.gov.au/images/documents/privacy/privacy-law-reform/Public_schedule_for_privacy_law_reform_guidance.pdf>; *APP Guidelines* above n 528.

will start to move from the broad guidance which has been issued to date, for example the new *APP Guidelines,*[532] to guidance dealing with specific areas and issues, based on specific business practices and feedback from all entities.[533]

The guidance documents published by the OAIC carry a disclaimer confirming they are not binding on the Commissioner. [534] Individual documents also state they are based on the OAIC's understanding of how the *Privacy Act* works and are intended to provide explanations of some of the terms used in the NPPs and good practice or compliance tips. In effect, they are intended to help organisations apply the NPPs in ordinary circumstances.[535]

This chapter will first consider the guidance documents issued by the Commissioner regarding NPP 4. The Commissioner also issues case notes and OMI reports providing details of its investigations. These publications can also be regarded as guidance and, to the extent they refer to NPP 4, are considered later in this chapter.

## 6.2 NPP 4 GUIDANCE

Guidance issued in relation to NPP 4 includes the *Guidelines to the National Privacy Principles* (2001)[536] and *Information Sheet (Private Sector) 6 – Security and Personal Information (Information Sheet 6).*[537] *Information Sheet 6* was superseded by a new *Guide to Information Security*[538] in April 2013, and is no longer published

---

532 *APP Guidelines* above n 528.

533 Timothy Pilgrim, Privacy Commissioner 'Privacy Reform – Act Three' (Presentation to the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013) < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>.

534 See, eg, Office of the Privacy Commissionere, ' Information Sheet (Private Sector) 30 - 2010: ID scanning in clubs and pubs' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-30-2010-id-scanning-in-clubs-and-pubs>.

535 Ibid.

536 Office of the Federal Privacy Commissioner, 'Guidelines to the National Privacy Principles' (2001) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guidelines-to-the-national-privacy-principles> ('*Guidelines to the NPPs'*).

537 Office of the Federal Privacy Commissioner, 'Information Sheet (Private Sector) 6 – Security and Personal Information' (2001) ('*Information Sheet 6*').

538 *Guide to Information Security*, above n 63.

on the OAIC's website. However, *Information Sheet 6* remains relevant to this research because it was the most specific guidance document available at the time of the 6 investigations that are considered in more detail in Part 3.

The *Guidelines to the National Privacy Principles* were published in 2001 following the introduction of the new NPPs. These guidelines contain three pages of guidance in regard to NPP 4, one and a half pages of which relate to destruction or de-identification for the purposes of NPP 4.2. They state that security could consist of maintaining physical security, computer and network security, communications security and personnel security. They then state that what is reasonable will depend on factors such as the sensitivity of the personal information held, the harm that could arise from its compromise, how the organisation stores, processes and transmits the personal information (for example, paper-based or electronic records) and the size of the organisation (the larger the organisation, the greater the level of security likely to be needed). The guidelines then list some of the steps which an organisation could take to ensure compliance, including:

- Identifying the security risks to personal information held by the organisation and the consequences of a breach of security;
- Developing a policy that implements measures, practices and procedures to reduce the identified risks to security;
- Training staff and management in security awareness, practices and procedures;
- Monitoring compliance with the security policy, periodic assessments of new security risks and the adequacy of existing security measures;
- Referring to Australian and international standards as a guide; and
- Depending on the size of the organisation and the information it collects, perhaps having an external privacy audit conducted.[539]

*Information Sheet 6,* also released in 2001, adopts the same general approach to compliance with NPP 4 but provides more detailed guidance. *Information Sheet 6* is

---

[539] *Guidelines to the NPPs*, above n 536, 45.

made up of two parts, the first titled 'Reasonable Steps' and the second titled 'Aspects of security to consider'. In the first section, it is noted that what is 'reasonable' is context dependent, and refers to a number of factors to be considered, such as the sensitivity of the information and the cost of the mitigation. In the section headed 'Aspects of security to consider,' *Information Sheet 6* lists a range of security measures, within the same domains as referred to in the *Guidelines to the NPPs*: physical security, computer and network security, communications security and personnel security. Examples of some of the 'range of security measures' within each those headings are given, as are 'tips for compliance' which include the use of standards such as ISO 17799 (now ISO 27002) and AS7799.2 (now ISO 27001).

As in the *Guidelines to the NPPs*, *Information Sheet 6* does not clearly link the selection of security measures to contextual factors or to outcomes of a risk assessment. There is reference to the need to assess security risks and then to take 'appropriate measures' but this is only in regard to 'computer and network security' and perhaps less explicitly in relation to 'communications security.[540]' In relation to specific controls, there is the occasional link between the suggested measure and risk, for example, the reference to 'encryption of data for high risk transmissions' as part of communications security,[541] but this is not part of any recommended process or method for the identification of the appropriate control to implement. However, the noting of contextual factors such as the sensitivity of the information and the costs of any security systems referred to as being pertinent to the assessment of 'reasonableness'[542] is akin to risk assessment (although not couched in the language of risk). In information security practice, these contextual considerations would be part of the risk assessment and treatment process underpinning the selection of the specific controls and the design of the overarching management system. For example, the sensitivity of the information would be relevant to the assessment of the consequences of breach (as part of the risk identification and assessment phase) and

---

[540] *Information Sheet 6*, above n 537, 2 – 3.

[541] Ibid 3.

[542] *Information Sheet 6*, above n 537, 1.

costs of the control would be relevant to a consideration of the appropriate risk mitigation in the risk treatment phase. The failure to explicitly link the selection and management of controls to the risk process is a significant departure from an industry practice approach to information security,

Monitoring and review are not identified as core requirements of an effective management system. Monitoring is referred to only in the context of compliance with information security policies[543] and the operation of network controls.[544] Moreover, *Information Sheet 6* does not refer to any governance around the implementation and operation of the security measures, which would ensure those measures are both appropriate and operating correctly.

The descriptions of the types of controls that come within the broad categories of computer and network and communications security could be regarded as high level and incomplete. Computer security measures referred to include access controls (such as passwords), virus checking, and IT support to deal with security risks, auditing procedures and data integrity checks.[545] Suggested communications security controls include checking facsimile numbers before transmission and authenticating identity before giving information over the phone. Other listed controls include encryption of data for high-risk transmissions. Reference is also made to network security which could include firewalls, routers, network intrusion detection systems, host intrusion detection systems, appropriate encryption and expert monitoring.[546] There is little description of what might be required for the effective implementation of each of these controls or how that might be used in combination. For example, should passwords be made up of a minimum number of characters, should they be a mix of alpha-numeric and symbols, should they be able to be re-used, should they be changed after a certain time? Perhaps not surprisingly as this guidance was issued in 2001, there are important areas not covered by the guidance. For example, no reference is made to ensuring the security of software and

---

543 Ibid 1.

544 Ibid 3.

545 Ibid 2- 3.

546 Ibid 3- 4.

web-facing applications, issues with the use of mobile devices or the use of third parties to provide support services or outsourced processing or to ensuring data recovery in the case of a disruption of operations.

In addition to these *Guidelines* and the *Information Sheet*, NPP 4 is referred to in each of the following publications:

- *Privacy Impact Assessment Guide* (Issued first in 2008 and revised in May 2010 and again in May 2014);[547]
- '*Privacy fact sheet 7: Ten steps to protect other people's personal information*;'[548]
- '*Privacy fact sheet 8: Ten steps to protect your personal information*;'[549] and
- '*Data Breach Notification: Guide to Handling Personal Information*.'[550]

Generally, each of these publications adopts the same approach as *Information Sheet 6*, although each publication refers to different controls that could be implemented.

The use of the guidance function specifically in relation to NPP 4 was considered by the ALRC, where it recommended a stronger guidance role for the Privacy Commissioner in regard to what is meant by 'reasonable steps.'[551] In terms

---

547 Office of the Australian Information Commissioner, 'Guide to undertaking privacy impact assessments (May 2014) '< http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments>, ('*Guide to undertaking privacy impact assessments*').

548 Office of the Australian Information Commissioner, 'Privacy Fact Sheet 7 Ten Steps to protect other people's personal information' (April 2012) <http://www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet7_10steps_protect_personal_info.html>.

549 Office of the Australian Information Commissioner, 'Privacy Fact Sheet 8 Ten Steps to protect your personal information' (April 2012) <http://www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet8_10steps_protect_your_information.html>.

550 Office of the Australian Information Commissioner, *Data Breach Notification: A guide to handling personal information security breaches* (April 2012) <http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html> ('*Data Breach Notification Guide'*).

551 *For your information,* above n 32, [28.26-28.30] [28.34] – [28.36].

of that guidance, the ALRC recommended that the Commissioner not 're-invent the wheel' but that the Commissioner's guidance should complement other existing guidance, such as the Protective Security Manual.[552] The ALRC also recommended that the Privacy Commissioner be empowered to establish expert panels that could be consulted on the implications of technological developments for data security or be used to develop education and guidance materials.[553] This is consistent with the encouragement provided by the ALRC to the growth of 'compliance professionals' and networks and more consistent dialogue between the regulator and the regulated entities, in order to provide a constant update on compliance levels in industries.[554]

The ALRC did not undertake any extensive investigation of the guidance issued at that time in relation to NPP 4[555] nor of the way that the Commissioner had referred to that guidance in NPP 4-related investigations prior to the release of the ALRC report.

The ALRC considered the extent to which the Commissioner could be expected to issue guidance in regard to technological developments. In response to that issue the Commissioner had indicated that it was concerned about the specialised level of expertise required to provide such guidance, along with the resource implications of continually ensuring the accuracy of guidance in a rapidly changing technological environment.[556] The ALRC acknowledged those concerns but suggested there were a number of ways of dealing with those such as referring readers to other sources of information including relevant international and national

---

552 Ibid [28-34]. The Protective Security Manual has been replaced by the Protective Security Framework and other supporting documents which have been discussed in more detail in Chapter 3.4.1.

553 Ibid Recommendation 28–3, 951. The right for the Commissioner to appoint expert panels was included in s27(3) of the Privacy Amendment Act.

554 Ibid [4.65] – [4.68].

555 IP 31 [4-115], where it was noted that the Office of the Privacy Commissioner had 'issued an Information Sheet' (albeit in 2001).

556 Ibid [28-28].

standards, without endorsing them.[557] Consequently it recommended that the OPC should provide guidance on relevant technological developments.[558]

Some five years after that recommendation, and twelve years after *Information Sheet 6*, the OAIC released a new *Guide to Information Security*.[559] As this *Guide* was published after the completion of the investigations considered in Part 3 of this research, it is not relevant to the detailed analysis of those investigations. However, the new *Guide* is relevant as a reflection of the Commissioner's latest thinking on NPP 4 and for that purpose it is considered further below.

### 6.2.1 Guide to Information Security

In their interviews, both the Commissioner and the Assistant Commissioner Compliance expressed the view that the *Guide to Information Security* represents the OAIC's current thinking as to what are reasonable steps for the purposes of NPP 4.[560] The Privacy Commissioner has also stated that the *Guide* 'will send a clear message about my expectations in this area' and that the OAIC would refer to it when assessing compliance with the data security obligations in the *Privacy Act*.[561]

The *Guide* applies to all entities covered by the *Privacy Act*.[562] Although stated to be non-exhaustive, the *Guide* also states that the OAIC will refer to it 'when assessing an entity's compliance with its security obligations in the *Privacy Act*.'[563]

The *Guide* is divided into three main sections:

- Information security;
- Circumstances that affect reasonable steps; and

---

557 Ibid [28-35].

558 Ibid [28-36].

559 *Guide to Information Security* above n 63.

560 Interview with Acting Commissioner Compliance, 14 December, 2012.

561 See, e.g. Timothy Pilgrim, Privacy Commissioner, 'Update your privacy setting' Presentation by to the Communications and Media Law Association, Sydney, 7 March 2013

562 *Guide to Information Security*, above n 63, 1.

563 Ibid.

- Steps and strategies which may be reasonable to take.

This structure is similar to *Information Sheet 6*, albeit with a new introduction section. The bulk of the guide is made up of the last section, which includes a much longer list than included in previous guidance, which only referred to physical security, computer and network security, communications security and personnel security. The new *Guide* now includes reference to Governance, Data Breaches, the Information Life Cycle, Standards and Regular Monitoring and Review.[564] Additional measures have been included in the section headed ICT Security (previously 'Communications and Network Security') such as Whitelisting or Blacklisting.[565]

Given the focus of this research on the relationship between industry practice and the manner that the Commissioner has exercised its powers in regard to NPP 4, the *Guide to Information Security* will be assessed by reference to the three-part industry practice approach that has been used as the basis for this research.

#### 6.2.1.1 Risk

Perhaps the major issue with the Guide is its treatment of risk. Not only is there no clear establishment of risk as the basis for the selection and implementation of controls, risk is used in a manner that indicates that the Commissioner may equate the term 'risk' with 'harm.' The *Guide* includes a section titled 'Risk to personal information'[566] that was called 'Protecting Personal information' in the consultation draft.[567] Rather than discuss how the risk assessment process should be used to identify threats and vulnerabilities in the context of the particular organisation and to then support the selection and management of appropriate security controls, the section simply lists some common situations that give rise to potential harm to

---

564 Ibid 15 – 28.

565 Ibid 4.

566 Ibid 7.

567 Office of the Australian Information Commissioner 'Guide to information security Consultation draft – December 2012' < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security> 5.

information assets. This view of risk in the limited context of 'risk of harm' ignores the importance of consideration of the likelihood of occurrence as part of risk prioritisation and the broader role of risk as part of a risk management based-information security management system.[568]

Following this section are two sections titled 'Privacy and your business' and 'Privacy by design, privacy impact assessment and information security risk assessments' (with the reference to information security risk assessment included after the consultation period).[569] These sections treat risk and information security as part of 'data handling practices' which should have privacy 'built in' through the use of Privacy by Design, which in turn can be achieved by conducting a Privacy Impact Assessment (PIA). Information security risk analysis is seen as a possible requirement for the completion of a comprehensive PIA:

> To inform the analysis of personal information security in the PIA, entities may need to conduct a more detailed information security risk assessment in conjunction with a PIA.[570]

It also states that any such PIA and information security risk assessments 'would inform the development of entity's risk management or information security plans.'[571]

It is not within the scope of this research to consider the principles of Privacy by Design in detail.[572] However, it is unlikely that the end to end design approach underpinning Privacy by Design would be achieved solely by a PIA which is a 'point

---

568 This confusion in the use of the term 'risk' was noted in the submission in response to the draft Guide by Standards Australia in Standards Australia 'OAIC Consultation Submission: Guide to Information Security: 'Reasonable steps' to protect personal information' 4 January 2013 < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security-reasonable-steps-to-protect-personal-information-consultation> , 5.

569 *Guide to Information Security* above n 63, 7 – 9.

570 Ibid 6.

571 Ibid.

572 See, e.g. Ann Cavoukian, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (IGI Global, 2012) 170.

in time' assessment, usually of a system or a business process.[573] Conducting a detailed information security risk assessment as part of a PIA for a new system or business process is certainly a prudent measure to take. Nevertheless, a PIA by itself is unlikely to ensure that appropriate information security controls are in place throughout the organisation. As discussed in Chapter 3, information security involves a complex system of layered controls across an organisation. Identifying the particular security requirements of a particular system or process in isolation of that broader organisational context is unlikely to achieve that goal.

The introduction of concepts such as Privacy by Design into a consideration of information security obscures the scope and purpose NPP 4. In NPP 4, the harms to be protected against are listed and include unauthorised disclosure or access, misuse and loss. NPP 4 does not extend to ensuring the proper operation of all aspects of privacy, such as the right to access or the right to correct personal information. These rights are part of the broader function of Privacy by Design.

From an industry practice point of view, the OAIC view of information security as an enabler of privacy and of risk assessment as, at best, an optional component of a PIA (something that entities 'may need to conduct') is problematic. This view of information security could not be regarded as reflective of industry best practice. In addition, the reference to the results of the PIA and the security risk assessment as informing the development of the entity's risk management or security plan suggest the sort of inappropriate conflation of privacy and security referred to in Chapter 1.

#### 6.2.1.2 Selection of Controls

Other than in a very general manner, the *Guide* does not link risk assessment to the selection of controls. As noted, it does refer to information security risk assessment in the context of a Privacy Impact Assessment as a process that 'identifies and evaluates threats and vulnerabilities,' which 'would inform the

---

573 See, eg, *Guide to undertaking privacy impact assessments'* above n 547 which defines a privacy impact assessment as "a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact."

development of entity's risk management or information security plans' and which also examines the 'adequacy of an entity's information security measures in mitigating the risks to information held by the entity (including personal information) and whether those risks should be further mitigated.'[574] Given these references, it might be expected that measures listed in the section 'Steps and strategies which may be reasonable to take'[575] would be prefaced by reference to an information security plan or the outcomes of a risk assessment. However, that link is not made.

Issues identified with the manner in which the security controls were described in the old guidance remain in the new *Guide*. Although not expressed to be exhaustive, there are important security measures missing. For example, the section on access controls focuses on passwords only and there is no reference to asset classification.[576] The *Guide* also uses a confusing format, posing a series of questions after making high-level statements of control objectives or definitions.[577] The *Guide* does not indicate the relevance of the answers to the questions (should they all be answered 'yes' for there to be reasonable security?) nor how those answers should be derived or what the consequence of the response might be. This format is not typical for information security guidance documents.[578]

---

574 *Guide to Information Security* above n 63, 6.

575 Ibid 15 – 28.

576 The omission of security measures and the need to clarify others was noted in submissions on the draft Guidance by the Australian Government Information Management Office (email from Glenn Archer to Dimitrios Kormas dated 21 January 2013 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/AGIMO_response_draft_Information_security_guide.txt>), the Australian Information Security Association (AISA 'The AISA Response to the Office of the Australian Information Commissioner's Guide to information security Discussion Paper' 7 January 2013) and Standards Australia.

577 See, eg, the section on "Testing" which notes that testing may take a number of forms and may be done internally or contracted out. The *Guide* then poses questions including: How often is testing conducted? Who is responsible for conducting testing? How is test data handled? If testing identifies weaknesses, how is this reported and address. *Guide to Information Security* above n 63, 21.

578 See, eg, Section 4 onwards of ISO 27002 which provides a description of the overall objective of the suggested security measure, defines specific controls that might be considered to meet that objective and then gives detailed implementation guidance as to how those controls might be designed and implemented.

As recommended in the ALRC report, the Commissioner's *Guide* refers more explicitly to relevant standards. In a section headed 'Standards' the *Guide* says '[e]ntities should consider using relevant international and Australian standards on information security to inform their risk based assessments of threats and vulnerabilities' and refers to the ISO 27000 series and to AS/NZS ISO 31000 of risk management standards. This wording and the reference to ISO 31000 (which is a generic risk management standard) could be interpreted as limiting the relevance of the ISO 27000 series to informing the risk assessment process, rather than as providing the specification for an information security management system supported by a code of practice (the intended purpose of ISO 27001 and 27002). This more limited recommendation regarding the use of standards may not be what the ALRC anticipated.

#### 6.2.1.3 Continuous Improvement Cycle

The *Guide* does recognise the importance of an iterative continuous improvement process. A section titled 'Managing the information life-cycle' was added to the *Guide* following the consultation period. Continuous improvement is also referred to in the 'Workplace Policies' section[579] and in a single paragraph section headed 'Regular monitoring and review,' added following the consultation period, which provides that entities should 'regularly monitor the operation and effectiveness of their ICT security measures.'[580] This is an important addition to the guidance, although it does sit uneasily with the other recommended security measures and is not identified as an essential part of any approach to managing information security.

#### 6.2.1.4 Consultation Process

The *Guide* was issued in late April 2013, following a one month consultation period between mid-December, 2012 and mid-January, 2013.[581] This short time

---

579 *Guide to Information Security above n 63*, 20.

580 Ibid 23.

581 Ibid.

frame provided limited opportunity for extensive consultation on the proposal. Notwithstanding this, at least 24 submissions were lodged.

The absence of a risk-based framework for the selection of controls was raised in most of the submissions. Lockstep Consulting submitted that the *Guide* should use the conventional method of risk assessment as the unifying framework or theme.[582] Similarly, the AGIMO recommended that the guidance should be set in the context of overall risk management, saying that 'there is no contextualisation from a risk perspective of any of the steps and strategies or the questions posed in the document.' The National Archives of Australia supported the approach taken by the ISM whereby 'risk is provided as context for the various controls.'[583]

Similarly, a number of submissions referred to the need for continuous monitoring and review: NEHTA submitted that an 'entity's practices of regularly reviewing security to ensure that the measures it adopts meet the needs of the changing technology landscape' should be considered as part of an investigation into NPP 4, and this should be stated in the *Guide*.'[584] McAfee referred to the need to 'implement a data governance program, measure its effectiveness, and test it on an ongoing basis to ensure that it remains successful over time.'[585]

These concerns were addressed to some extent in the final draft, with the inclusion of the various references to risk that have already been discussed (none of which appeared in the original *Guide*) and the section titled 'Regular Monitoring and

---

582 Letter from Lockstep Consultant to Ms Angelene Falk, Acting Assistant Commissioner Compliance, 8 January 2013 < http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/Lockstep_response_draft_Information_security_guide.pdf>.

583 National Archives of Australia, 'Comments on Draft Guide to Information Security' <http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security-reasonable-steps-to-protect-personal-information-consultation>.

584 NEHTA, 'Submission to the Office of the Australian Information Commissioner', 8 January 2013 < http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/NeHTA_response_draft_Information_security_guide.pdf>

585 Email from Michael Morgan to Office of the Australian Information Commissioner, 14 January 2013 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/McAfee_response_draft_Information_security_guide.txt>

Review.'[586] However, as discussed, these inclusions, particularly in regard to risk, are not entirely successful and largely fail to address the concerns raised in the submissions made in response to the draft. Between the closure of submissions and the publication of the final *Guide* there was no evidence of any further engagement in any regulatory conversation regarding the terms of the final document. The submissions themselves were not published until after the release of the final version of *Guide*.[587]

### 6.2.2 APP Guidelines

Final guidelines regarding the Commissioner's interpretation of the new APPs were released in February 2014. These guidelines include guidance on APP 11 (which replaces NPP 4) in Chapter 11.[588] This guidance is not dissimilar to that provided in the superseded *Guidelines to the NPPs*. For the purposes of this research, the relevant part of the guide is headed 'Taking Reasonable Steps' and refers to the need to consider relevant circumstances listing the same contextual factors as appeared in the previous guidance.[589] It refers to some of the steps and strategies that may be reasonable to take, under the same headings as used in the *Guide to Information Security*, and finishes by directing readers to that *Guide* for 'further discussion of the relevant considerations, and examples of steps that may be reasonable for an APP entity to take.' [590] Under the heading 'What are the security considerations?' it provides explanations of the different behaviours that the principle refers to, such as interference, unauthorised access etc.[591]

---

586 *Guide to Reasonable Security*, above n 63, 28.

587 Submissions were made by the author and other parties to the knowledge of the author, including the Australian Information Security Association and the Australian Privacy Foundation.

588 Office of the Australian Information Commissioner, 'Chapter 11:APP 11- Security of Personal Information', February 2014, <http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/chapter-11-app-11-security-of-personal-information>.

589 Ibid [11.7] – [11.9]

590 Ibid [11.9].

591 Ibid [11.10] – [11.18].

Similar to the issues identified above in regard to the *Guide to Information Security*, there is no reference to risk assessment, nor is there any linking of the risk assessment results to the selection of controls from the list of 'steps and strategies.' There is no reference even to the high level concepts such as Privacy by Design which are used to frame the discussion of risk in the new *Guide to Information Security*. As a consequence, the APP guidance does not materially add to the guidance provided in the more detailed *Guide to Information Security*.

The extent to which the OAIC's published guidance is referred to in the Commissioner's investigations is considered in more detail in the consideration of issued case notes and OMI reports below and in the review of the Commissioner's use of its investigation powers in Part 3 of this research.

### 6.2.3 Analysis

Although improved as a consequence of the consultation process the most recent *Guide to Information Security* still has many issues, particularly in its failure to align its interpretation of reasonable steps with risk-based information security management practice, the high-level nature of the information provided in regard to the specific security measures that may be taken, the omissions from the list of recommended security measures and the lack of emphasis of the importance of on-going monitoring and review as part of an over-arching governance process. Accordingly, it is difficult to regard the *Guide* as entirely consistent with standard information practice.

In terms of transparency, balance and vigour:

- The twelve year gap between the issuing of guidance in regard to what is one of the most important issues affecting the protection of personal information suggests a lack of vigour;
- There was only limited transparency in the consultation process preceding the release of the new *Guide to Information Security*. Submissions were not published until after the release of the *Guide* and it is not clear that further consultation occurred on the basis of those submissions;
- It could be argued that the high-level nature of the advice provided in the *Guide* means there is still little transparency regarding the Commissioner's

expectations in terms of compliance with NPP 4. This lack of specificity could reflect concerns about the advice becoming dated with the rapid change of technology[592] and the associated resource issues for the OAIC in keeping the advice current.[593] Whatever the reason, the lack of specificity impacts the effectiveness of the guidance provided.

## 6.3 GUIDANCE ON INVESTIGATIONS

Guidance has been issued by the OAIC in regard to how it conducts investigations. This includes two Information Sheets issued in 2008: one explaining the conciliation of privacy complaints[594] and the other providing a step by step guide on how to conduct an internal investigation.[595] More recently, the Commissioner released new fact sheets explaining the processes the OAIC itself uses in its response to complaints, providing guidance on how to conduct internal investigations and more information on the OAIC's conciliation process.[596] The OAIC had also published its '*Privacy Complaints and Procedures Manual*' (*Complaints Manual*)[597] although this document is no longer published nor archived on the OAIC's

---

592 *For your information,* above n 32, [28-28], [28-36] where the ALRC refers to the OPC concerns regarding the skills and resources required to issue guidance on relevant technological developments. See also Jackson and Shelly, above n at 129.

593 Ibid [28-28].

594 Office of the Australian Privacy Commissioner, 'About the Office Information Sheet - Conciliation of Privacy Complaints' (February 2008) .

595 Office of the Privacy Commissioner, 'Public Sector Information Sheet 2 - A step by step guide to internal investigations of privacy complaints by Australian and ACT government agencies' (August 2008).

596 Office of the Australian Information Commissioner, 'Privacy Fact Sheet 9: Guide to Internal Investigation', (April 2012) < http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-9-guide-to-internal-investigations>; Office of the Australian Information Commissioner, 'Privacy Fact Sheet 10: What will happen to my complaint?', (June 2012) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-10-what-will-happen-to-my-complaint>; Office of the Australian Information Commissioner , 'Privacy Fact Sheet 11: How will the OAIC handle a privacy complaint against my organisation', (June 212) < http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-11-how-will-the-oaic-handle-a-privacy-complaint-against-my-organisation > ('*Fact Sheet 11*').

597 *Complaints Manual*, above n 227.

website.[598] The extent to which the *Complaints Manual* is followed in the conduct of investigations is considered further in Part 3 in the context of the OAIC's use of its investigation powers.

## 6.4 CASE NOTES AND OMI REPORTS AS GUIDANCE

Summaries of investigations conducted by the OPC and the OAIC are published in the form of either case notes, which relate to complaint-based investigations, or OMI reports that relate to own motion investigations. The same principles apply to the publication of OMI reports as apply to the publication of case notes.[599] Each provides a synopsis of the case under consideration rather than a comprehensive record of the proceedings.[600] Neither case notes nor OMI reports are intended to be legally binding or to provide legal advice.[601] According to the *Guide to Producing Case Notes*, case notes are intended to 'illustrate how the privacy principles apply in common sets of circumstances, or how the OAIC interprets aspects of the Act' and will also 'illustrate the OAIC's complaint handling process in relation to complex or difficult investigations.'[602] The *OAIC 2012 Annual Report* states that the purpose of publishing case notes is to provide an insight into how the NPPs are being applied which can, among other things:

- Encourage good privacy practices and compliance with the *Privacy Act*; and
- Demonstrate accountability and transparency in the OAIC's processes and decision-making.[603]

---

598 Ibid.

599 *Guide to Producing Case Notes,* above n 248, 1 which provides that 'case notes can include own motion investigations (OMIs) to illustrate the circumstances that led to the OMI and how it was resolved.'

600 Office of the Australian Information Commissioner, 'Privacy case notes' <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-case-notes>.

601 Ibid.

602 *Guide to Producing Case Notes,* above n 248, 1-2.

603 *OAIC 2012 Annual Report*, above n 1, 65.

Similar comments are included in the *OAIC 2011 Annual Report*.[604] There are no references to case notes in the *OAIC 2013 Annual Report*, which may be a consequence of there being no case notes published in the period covered by that report.

The Commissioner's website does not provide any reasons for the publication of OMI reports. However it does state that OMIs 'may look at a specific act or practice, at a systemic problem or recurring pattern in an entity's practices and processes in handling personal information, or at a practice or problem occurring in more than one entity.'[605] Given that the *Guide to Producing Case Notes* considers OMI reports to be the same as case notes,[606] it is assumed that OMI reports are published for the same reasons as apply to the publication of case notes.[607] Accordingly, the publication of case notes and OMI reports could be considered part of the exercise of the Commissioner's guidance power, certainly to the extent that publication is intended 'to help organisations and the community understand the way the Office applies the provision of the Act.'[608]

There are two other possible reasons for the publication of case notes and OMI reports, namely, transparency of compliance activities; and deterrence. These are considered further in Part 3 of this research.

In 2001, the Commissioner published its *Guide to Producing Case Notes* which confirmed that the OPC would publish more frequent, de-identified case notes on complaints it had handled.[609] Prior to that time, public reporting on the Commissioner's use of its investigation powers was done via the inclusion of short summaries of cases in the OPC's annual report.

---

604 *OAIC 2011 Annual Report,* above n 1, 26.

605 Office of the Australian Information Commissioner, 'Commissioner initiated investigation reports' < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

606 *Guide to Producing Case Notes,* above n 248, 1.

607 See the discussion of the reasons for publishing case notes included in Chapter 7.1.4.

608 *Fact Sheet 11*, above n 596.

609 *Guide to Producing Case Notes,* above n 248 , 3.

The *Guide* also provided a series of rules for the style and format of reporting.[610] These include that case notes should be concise and contain only the information necessary to demonstrate the relevant point of law, view, or successful outcome. The *Guide* suggests that the average case note should be between half a page and one page in length, although more complex cases may require up to two pages.[611] The *Guide* also attaches a template for case notes.[612] That template divides the report into four sections: Law, Facts, Issues and Outcome.[613] The *Guide* suggests that the Outcomes section should cover the action taken by the Commissioner as well as the view formed and the ultimate resolution. However the example Outcome section given is contained in a single sentence which provides: ''The Commission formed the view that the act or practice may have been an interference with privacy, but declined to investigate further on the grounds that the respondent had dealt adequately with the complaint.'[614] By contrast, the Outcome section in the case note template provides a more detailed basis for the outcome, referring to the facts and applying the relevant principles to those facts.[615]

From 2002 until February 2011, the format of all case notes and OMI reports was consistent with the OAIC's *Guide to Producing Case Notes*:

- They were short, most being no more than one page. Most reports were around 500 words, although one OMI report had only 396 words;[616] and
- They were divided into four main sections headed 'Facts', 'Issues' and 'Outcomes' after identifying the relevant principles being considered under the heading 'Laws.' The Outcome section in each case note includes any

---

610 *Guide to Producing Case Notes,* above n 248, 7.

611 Ibid.

612 Ibid 9 -10.

613 Ibid.

614 Ibid 6.

615 Ibid 11.

616 *Own Motion Investigation v Information Technology Company* [2010] PrivCmrA 24.

decision as well as some indication of the basis on which the case was closed.[617]

From 2002, the OPC also adopted a new form of complaint report citation and agreed that the complaint report summaries could be republished on the AustLII website in addition to its own website.[618]

*Table 4* shows the number of case notes and OMI reports published each year between 2008 and 2013, together with the number of OMIs undertaken. The information is taken from the OPC and OAIC annual reports and the OAIC website.

| | 2008- 2009 | 2009 - 2010 | 2010- 2011 | 2011 - 2012 | 2012 - 2013 |
|---|---|---|---|---|---|
| **No of case notes issued (Annual Report)[619]** | 18 | 27 | 22 | 14 | Not reported |
| **No of case notes (OAIC Website)[620]** | 8 | 23 | 19 | 8 | 0 |
| **No. of investigations** | 83[621] | 73[622] | 59[623] | 37[624] | 13[625] |

617 *Guide to Producing Case Notes,* above n 248.

618 Greenleaf, 'A proposal for improving accountability of Asia-Pacific Privacy Commissioners', above n 65, 8 – 9.

619 The number of published case notes for the years from 2008 – 2010 include the OMI reports and case notes from complaint investigations. The details are included in the *OAIC 2012 Annual Report*, above n 1, 65; *OAIC 2011 Annual Report*, above n 1, 33; *OPC 2010 Annual Report*, above n 403, 64; *OPC 2009 Annual Report*, above n 1, 68.

620 The number has been collated based on the reports published on the OAIC website and Austlii. A list of all case notes published between July 2008 and June 2013 is included in Appendix A. Investigation Reports are published on Austlii at <http://www.austlii.edu.au/au/cases/cth/PrivCmrA/>.

621 *OPC 2009 Annual Report*, above n 1, 70.

622 *OAIC 2010 Annual Report*, 66.

623 The *OAIC 2011 Annual Report,* above n 1, refers to '59 new matters involving alleged interferences with privacy were assessed for investigation as OMIs' at 36. Table 5.15 shows

| | | | | | |
|---|---|---|---|---|---|
| **(OMIs)** | | | | | |
| **No. of OMI reports (Annual Report)**[626] | Not reported | Not reported | Not reported | 6 | 2 |
| **No of OMI reports (OAIC website)**[627] | 3 | 1 | 5 | 4 | 2 |

*Table 4: Case notes and OMI reports published by the OPC and the OAIC.*

Regardless of issues in reconciling the number of reports referred to in the Annual Reports and those published on the OAIC's website, it is clear that the number of published case notes has been in decline since 2010 – 2011.[628] The high point for the publication of OMI reports was the following year, 2011 – 2012. Since then, the number of published case notes, the number of OMIs conducted and the number of OMIs reported has all dropped considerably. Two OMI reports were published in July 2012[629] which related to investigations commenced in the previous year. No further report was published until some 15 months later when the

that NPP4 was an issue raised in 37 OMIs opened in 2010 -201, and IPP 4 was relevant in another 2 OMIs.

624 *OAIC 2011 Annual Report*, above n 1, 62.

625 *OAIC 2013 Annual Report,* above n 381, 77.

626 The details are included in *OAIC 2013 Annual Report,* above n 381, 62 and *OAIC 2012 Annual Report*, above n 1, 77.

627 The number has been collated based on the reports published on the OAIC website and Austlii and details of all of the published OMI reports are included in Appendix B.

628 This drop might be attributable to the increased OMI reporting during that period, which is discussed further below.

629 *Medvet OMI Report*, above n 341, and *Telstra Bundles OMI Report*, above n 339.

*APPT/Melbourne IT Report*[630] was released in October 2013. Between October 2013 and March 2014, two more OMI reports were released.[631]

It is possible that the decrease in the number of reported own motion investigations, the number of own motion investigations actually undertaken and the number of published case notes is due to the OAIC's limited resources. The *2013 Annual Report* refers to an OAIC restructure that took place because of resourcing constraints, and the consequential reduction in own motion investigations and audits undertaken.[632] Resourcing issues affecting the way the Commissioner conducts investigations are discussed further in Part 3.[633] However, it also seems that the OAIC elected to pursue the investigation of high-profile data breach cases, notwithstanding the impact that had on its ability to conduct audits, carry out other investigations and issue case notes.[634]

The 2011 – 2012 year highpoint for publication of OMI reports coincided with a change in approach by the OAIC to OMI reporting. For the first time the respondents were named, the reports were considerably longer and in most cases the initiation of the investigation and the issuing of the reports were accompanied by OAIC-issued press releases.[635] The Commissioner publicly referred to this new approach noting the number of high profile data breach cases which had come to the office's attention together with the public interest in the Commissioner conducting an

---

630 Office of the Australian Information Commissioner, 'AAPT and Melbourne IT: Own Motion Investigation Report', (October 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/aapt-and-melbourne-it-own-motion-investigation-report>.

631 Office of the Australian Information Commissioner, 'Telstra Corporation Limited: Own Motion investigation report', (March 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014> and Multicard Pty Ltd: Own Motion Investigation Report (May 214) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/multicard-omi>.

632 *OAIC 2013 Annual Report,* above n 381, 11 – 12.

633 See Chapter 9.7.3.

634 *OAIC 2011 Annual Report,* above n 1 , 42 and evidence given as to the impact that investigations into data breach cases had on resources in Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing* (14 February, 2012), 41 – 43.

635 See the media reports referred to in n 940, 941.

investigation.[636] The reasons given for the new approach (in both speeches made by the Commissioner and the OAIC's annual reports) included the promotion of public confidence and the provision of transparency of regulatory activities.[637] All of these high profile investigations involved data security issues.[638] Given the different approach taken to these more recent 'high profile' OMIs, those OMI reports will be considered separately as part of the assessment of the Commissioner's use of its investigation powers in Part 3 of this research.

### 6.4.1 Case notes, OMI reports and NPP 4

Prior to 2013, the main difference between case notes and OMI reports, other than the reason for the investigation, was the frequency of publication, with fewer OMI reports published than case notes. 23 of the cases notes published between 2001 and 2013 involved some consideration of compliance with NPP 4. NPP 4 was considered in eight OMI reports between 2005 when the first OMI report was published[639] and February 2011.[640]

The reports deal with a range of different incidents giving rise to concerns about compliance with NPP 4. The most common complaint was the failure to prevent unauthorised access or disclosure (raised in a total of 19 of the 23 cases) followed by the loss of information (raised in six cases).[641] Unnecessary retention in breach of NPP 4.2 was raised in four cases

---

636 *OAIC 2011 Annual Report*, above n 1, Chapter 5, 5.

637 Privacy Commissioner 'Privacy: What's Ahead in 2012?' (Presentation to International Association of Privacy Professionals Australia & New Zealand Annual Summit, 30 November 2011) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-whats-ahead-in-2012>, *OAIC 2012 Annual Report*, above n 1, Chapter 6, 1; *OAIC 2013 Annual Report,* above n 381, 78.

638 Privacy Commissioner, 'Information security is now the major issue affecting consumer privacy' (Media Release, 29 April 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/information-security-is-now-the-major-issue-affecting-consumer-privacy>.

639 *OPC v Bank Institution* [2005] PrivCmrA.

640 A list of all the case notes and OMI reports which have considered NPP 4 is included in Appendix E.

641 Most cases have more than one cause for complaint so the total number of complaints raised is more than the total number of cases.

In the 23 relevant complaint-based investigations, the respondent was found to have breached at least one of the privacy principles in 10 cases. In all those cases where the Commissioner found there had been a breach, the Commissioner was able to close the investigation on the basis that the issue had been adequately dealt with (either by reaching a conciliated outcome with the complainant or the Commissioner forming a view that the respondent had adequately dealt with the complaint). This Commissioner's successful use of conciliation to close complaints is discussed further in Part 3.[642]

There were also few findings of breach of NPP 4 in any of the OMI reports. To the contrary, the Commissioner was able to conclude in most cases that the respondent was not in breach even where this required reliance on action taken by respondent after the incident had occurred. By way of example, in *Own Motion Investigation v Medical Centre*[643] medical records were stolen from a bin outside a medical centre and found in an adjacent park. The medical centre advised it was installing secure fencing around the premises, moving the medical waste bin inside the secured premises and fitting it with a new secure lock. New policies and procedures for secure destruction of personal information were developed and medical and administrative staff were trained in those procedures. The centre also obtained a shredder for secure on-site destruction. In view of those actions, the Commissioner was satisfied the medical centre had taken reasonable steps and had met the obligations imposed by NPP 4.1. The fact that those steps had not been taken prior to the incident does not seem to have been considered. A similar outcome was reached in *Own Motion Investigation v Airline*[644] where a computer glitch caused the disclosure of other travellers' details to a passenger checking in online. Given the processes that the respondent already had in place and that the code problem which led to the disclosure was remedied soon after the respondent was notified of the error, the Commissioner took the view that the steps taken to respond

---

642 See Chapter 7.1.2.

643 *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6.

644 *Own Motion Investigation v Airline* [2009] PrivCmrA 7.

to the error were adequate and closed the investigation into the matter, without any finding as to whether or not there had been a failure to comply with NPP 4.

There are exceptions to this. A telecommunications company offered a service whereby individuals could access their mobile phone account information by calling an 1800 number, following voice prompts and keying in the relevant mobile phone number.[645] The Commissioner found that the company was in breach of NPP 4 because anyone who knew an individual's mobile phone number and mobile carrier could call the 1800 number and access the individual's account balance without their authority. The company proposed to introduce additional authentication measures which satisfied the Commissioner and the investigation was closed

Generally the reports seem to suggest that the Commissioner's primary interest is in ensuring that issues are resolved, rather than considering the application of NPP 4 to the particular circumstances to determine whether or not the respondent was in breach. This is certainly consistent with the responsive regulation approach which supports non-punitive regulatory responses where the regulated organisation is voluntarily bringing itself into compliance. However, the focus on the remediation efforts taken, rather than on the steps which should have been taken in the first instance to comply with NPP 4, detracts from the transparency of the interpretation and application of the principle and consequently the guidance and educative value of the OMI reports.

### 6.4.2 Industry Practice

For the purposes of this research, it is important to determine the extent to which these reports could be regarded as supporting the industry practice approach to information security put forward in this research. As previously discussed, the industry practice approach to information security put forward by this research is comprised of three elements:

- The use of risk assessment (ideally via the identification of threats and vulnerabilities) as the basis for the identification of risks to information assets and the selection of security safeguards to manage that risk;

---

645 *Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16.

- The selection of security safe guards including administrative controls (such as policies and personnel related controls), physical and technical security controls to manage the risks identified; and
- The adoption of an iterative process-based approach that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks. [646]

Only four of the reports provide any statement of general principle as to the Commissioner's interpretation and application of NPP 4. However, in each of those cases, the statement of principles could be regarded as reflecting, at least in part, this industry practice approach.

In *D v Health Service Provider*[647] the complainant was asked to return to a private clinic because notes from the initial consultation could not be located. The complainant complained about the loss to the OPC. The respondent gave evidence that it believed that the single page of notes was probably in the complainant's possession and in any case did not contain any information that could identify the complainant. The case note provides that the decision as to what are 'reasonable steps' to ensure data security depends on a number of factors, such as the circumstances in which personal information is held. The sensitivity of personal information stored is also an important factor and higher levels of security could be expected for sensitive information, such as health information. In that case, in the absence of any evidence to the contrary, the Commissioner could not be satisfied that the missing sheet of paper contained any 'personal information' about the complainant and so decided to close the investigation. A similar statement was included in *S v Health Service Provider*, also published in 2008 and also involving a health service provider (the facts of which are considered further below).[648] A statement of principle in regard to NPP 4 in identical terms to that included in *D v*

---

646 See Chapter 3.4.

647 *D v Health Service Provider* [2008] PrivCmrA 4.

648 *S v Health Service Provider* [2008] PrivCmrA 19.

*Health Service Provider* and *S v Health Service Provider* was included in only one of the eight OMI reports *Own Motion Investigation v Medical Centre,*[649] the facts of which case have already been discussed. The reference in each of these three reports to relevant circumstances reflects at least the first part of an industry practice approach: the importance of considering risk or context.

In *E v Retail Organisation*[650] it is provided that protecting the security of personal information consists of maintaining computer and network security by adopting measures to protect computer systems and networks used for storing, processing and transmitting personal information, from unauthorised access, modification and disclosure. [651] This could be regarded as reflecting the second element of the industry practice approach: the need to select a range of controls to protect against all identified risks.

There are no similar statements of general principle in any of the other twenty case notes or seven OMI reports in which NPP 4 was considered.

#### 6.4.2.1 Risk

Risk is an integral part of an industry practice approach to information security. Accordingly, some consideration of risk or relevant circumstances might be expected in the reports dealing with NPP 4. The only case which makes specific reference to risk is *S v Health Service Provider*.[652] In that case, x-rays which were part of the complainant's medical history were lost in the mail. In determining whether the use of the mail was a breach of NPP 4 the case note refers to the significant harm that could be caused by the permanent loss of these records, the size of the organisation,

---

649 *Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6.

650 *E v Retail Organisation* [2007] PrivCmrA 7.

651 Ibid.

652 *S v Health Service Provider* [2008] PrivCmrA 19. *E v Financial Institute* also refers to risk but in the sense that the absence of access logging means that the organisation runs a greater risk of breaching NPP 2. There is also a reference to risk in *D v Commonwealth Agency* [2010] PrivCmrA 5 (31 May 2010), where the complainant was questioned by a government agency in the presence of journalists. The Commissioner considered that a high level of security was necessary given the high risk to the individual of third parties accessing the information. However, as this case involved a Commonwealth agency rather than a private entity, it is outside the scope of this research.

the cost of alternative delivery methods and the level of risk of records and x-rays being lost "in a generally dependable and reliable general mail system."[653] In view of these factors, it determined that the health service provider had not taken reasonable steps.

While not referring to "risk," a small number of cases refer to particular circumstances which might be considered to have some relevance to the determination of "reasonable steps." For example, the sensitivity and amount of information held were noted as relevant considerations in *N v Utility Provider*.[654] In that case, it was alleged that the complainant's ex-partner, an employee of the utility provider, improperly accessed the complainant's accounts in order to ascertain information about his assets. Although the Commissioner found there was insufficient evidence to conclude that there had been a breach of the *Privacy Act*, it did consider the application of the NPP 4 as the utility had not been able to provide any audit trail showing access to the complainant's information. The Commissioner noted that the utility provider held personal information of a large number of individuals and that the type of information required to establish accounts was extensive and that accordingly the information should be afforded a high level of protection, especially given the possible serious consequences for customers if there was unauthorised access to that information.[655]

The sensitivity of the information was also referred to in *E v Financial Institution*[656] which was another case where the complainant alleged that a staff member had accessed their personal information and disclosed it to a third party. The Commissioner suggested to the respondent that it may be reasonable to implement access controls in an environment where sensitive information, such as financial information, can be accessed by many employees throughout an organisation.[657] The case notes do not however support any consistent or systematic

---

653 *S v Health Service Provider* [2008] PrivCmrA 19, 1.

654 *N v Utility Provider* [2006] PrivCmrA 13.

655 Ibid.

656 *E v Financial Institution* [2003] PrivCmrA 3

657 Ibid.

approach to the consideration of relevant contextual issues as part of the assessment of reasonable steps for the purposes of NPP 4.

#### 6.4.2.2 Security measures

The second part of the industry approach to information security put forward in this research is the selection of security safe guards including administrative controls (such as policies and personnel related controls), physical and technical security controls to manage the risks identified as part of the risk assessment. Although the case notes do not support any systematic approach to determining the adequacy of the steps taken to protect information, the cases do seem to support a number of general propositions about the need for different types of security controls.

One such proposition is that some sort of access tracking should be in place. *E v Financial Institution*[658] was one of the first cases to raise the importance of having an enquiry audit trail to be able to track staff accesses to customers' personal information. The same point was made *in N v Utility Provider*[659] where the Commissioner considered the absence of access tracking 'in a large automated billing system' to be a failure to take reasonable steps.

Physical access controls for the storage of paper records have been referred to in a number of cases, usually in relation to missing medical records. [660] In one case where a file containing a child's complete medical history could not be located, possibly because of misfiling, the Commissioner was prepared to regard the incident as a one off human error rather than failure to take reasonable steps. [661] The respondent was able to provide information about its hard copy and electronic record management systems which included access controls, physical security measures and storage, archiving and shredding protocol, which the Commissioner regarded as evidence of taking reasonable steps. However, the basis on which the Commissioner

---

658 Ibid.

659 *N v Utility Provider* [2006] PrivCmrA 13

660 *D v Health Service Provider* [2008] PrivCmrA 4; *G v Counselling Service* [2009] PrivCmrA 9.

661 *V v Health Service Provider* [2006] PrivCmrA 21.

determined that an unauthorised access, disclosure, misuse or loss is the result of a systemic issue rather than a one off human error or vice versa is not entirely clear.

In *G v Counselling Service*[662] where one page of notes from a counselling session could not be located, the Commissioner considered the practice's procedures for securing client files both during and outside business hours and determined they were reasonable and the loss of the page of notes was a one-off human mistake rather than a systemic issue. There is no explicit assessment of the appropriateness of those procedures in the context of the possible consequences of the loss of information. In the case note, little detail is provided of the design of the actual systems in place having regard to the risk of loss or unauthorised access or disclosure, how those systems were implemented or operated or how compliance was being monitored and reviewed. In *V v Health Service Provider*[663] the Commissioner was of the view that the health service provider's record management policy, which included access controls, physical security measures and storage, archiving and shredding protocol, was reasonable. Again, although no detail is provided as to the basis for this determination, the Commissioner decided that the misplacement of the medical record was the result of human error and not the result of a systemic procedural problem on the part of the health service provider.[664]

Although the case notes may support some general propositions as to the security controls that should be in place, no framework for the assessment of appropriate security measures is provided. As discussed in Chapter 3, information security requires a complex system of inter-related controls of different types. The presence or absence of any particular control in isolation is unlikely to be authoritative as to whether reasonable steps had been taken to secure the personal information. Entities looking to the case notes for guidance on the security measures they should implement would be hard pressed to derive more than the most general advice.

---

662 *G v Counselling Service* [2009] PrivCmrA 9.

663 *V v Health Service Provider* [2006] PrivCmrA 21.

664 Ibid.

#### 6.4.2.3 Process-based approach

The adoption of an iterative process that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks is the third component of the industry practice approach to information security adopted in this research. This requirement has received little attention in any of the reports which have considered NPP 4. There is only one case where, although there were procedures to manage access control, the Commissioner determined that the failure to ensure that these controls were consistently applied meant that there was a failure to take reasonable steps [665] Evidence of the application or enforcement of policies and procedures has not been referred to in any of the other case notes.

#### 6.4.2.4 Guidance, industry standards and practice

It would be expected that explicit reference to the guidance discussed in Chapter 6.2 would be made in those case notes and OMI reports which have considered NPP 4. Not only would this be consistent with the purpose of the guidance but it also would be consistent with the investigation process set out in the *Complaints Manual* which refers to these documents and states that they 'represent the public position of the OAIC and should guide the application of the law to complaints.'[666] However, an analysis of those case notes and OMI reports where breach of NPP 4 has been considered shows no reference to any OAIC guidance, including the guidelines and information sheets referred to above. [667]

There are also few references to the elements identified in the OAIC's guidance as relevant to the assessment of reasonable steps (such as the size of the

---

665 *R v Internet Service Provider* [2005] PrivCmrA 17,

666 See Chapter 7.1.1

667 *L v Commonwealth Agency* [2010] PrivCmrA 14, relates to a breach of IPP 4 and includes reference to the *Plain English Guidelines to Information Privacy Principles 8-11* as providing examples of when an individual may be considered to be reasonably likely to be aware that information may be disclosed under IPP 11.1(a). No reference is made to any guidance relevant to IPP 4.

organisation or the amount of personal information held) or the different groups of security controls that may be selected. It is not clear why the case notes and OMI reports do not refer to the OAIC's own guidance. If the OAIC does not take its own guidance into consideration when applying the privacy principles, it is difficult to suggest that the regulated entities should have such regard. Inclusion of references to the existing guidance in case notes and OMI reports would also help clarify the application of that guidance to different facts and circumstances.

It is also pertinent to consider any references to industry standards (such as ISO 27001 and 27002) in the OAIC's case notes. Both *Information Sheet No 6* and the *Guidelines to the NPPs* recommend consideration of the use of industry standards as part of determining what might be reasonable steps.[668] In *P and Retail Company*[669] the Commissioner referred to relevant industry standards to determine if the collection of information was 'fair.' By contrast, there are few references to industry standards in the context of considering whether or not reasonable steps have been taken for the purposes of NPP 4. In *N and Utility Provider*, the case note states that 'the entity advised that it complied with the relevant Australian Standard and with its own procedures to ensure the security of personal information.'[670] Unfortunately, there is no further discussion of what this meant in practice. There was, for example, no interrogation into whether a risk assessment had been done to support compliance with the Standard (assuming it was ISO 27001 or one of the similar approaches to information security). Nor was there any discussion around whether adherence with the Standard would have required the implementation of access logs or audit trails of access to the entity's billing system. Without any more detailed consideration of what that compliance with the relevant Australian Standard meant, the reference to it in the case note is not helpful.

In addition to the limited reference to its own guidance and industry standards, no reference is made to the outcome of any other investigation by the Commissioner

---

668 *Guidelines to the NPPs*, above n 536, 45.

669 *P and Retail Company* [2011] AICmrCN 10.

670 *N and Utility Provider*, 1.

in any of the case notes. This is notwithstanding that the *Complaints Manual* provides that OAIC officers should take past decisions into account.[671]

### 6.4.3 Transparent, balanced and vigorous

It is important to consider the extent to which the reports considered above could be regarded as representing the appropriate use of powers by the Commissioner by reference to the principles of transparency, balance and vigour.

There are a number of case notes which clearly link the findings of fact, the reasons for the decision and the decision, providing transparency of decision-making. A good example is *S v Health Service Provider*[672] the facts of which have already been considered. The case note refers to the sensitivity of the medical records and x-rays, the harm to the complainant if they were lost and the resulting expectation that they should be afforded a higher level of protection than other forms of personal information. The Commissioner also considered the level of risk of the medical records and x-rays being lost in a generally dependable and reliable general mail system and noted that while respondent was not a large organisation, the cost of alternative methods to transmit the documents would not be a significant financial burden. Accordingly, the Commissioner's decision that the health service provider failed to take reasonable steps by using the general mail, in breach of NPP 4, is supported by the findings of fact which in turn are linked to the reasons for the decision.[673]

However, as discussed, in most of the reports detailed reasons for the determination as to the adequacy or otherwise of the steps taken to protect the information are not provided. An example is *H and Registered Club*[674] where the complainant raised concerned about the club using an identity card scanning machine to scan her driver's licence on entry to the club. The complaint was resolved through conciliation with the club agreeing to delete the data from the machine in return for

---

671 Ibid.

672 *S v Health Service Provide*r [2008] PrivCmrA 19.

673 Ibid 1.

674 *H and Registered Club* [2011] AICmrCN 2.

the complainant providing a statutory declaration including her address details. Concerns regarding the security of the information were addressed in the case note by a single sentence: 'The Commissioner also considered the security procedures and notice at the entrance of the club adequately dealt with that aspect of the complainant's complaint.'[675] The case note does not contain any general statement in regard to what is meant by 'reasonable steps' or what might be relevant factors in making that determination. There is no direct reference to the sensitivity or quantity of data being collected from patrons other than the complainant. The report provides no details as to the Club's security procedures or how the Commissioner was able to form the view that they were reasonable. Elsewhere in the report there is reference to the notice at the club entry which directs patrons to the registered club's privacy policy. It is not clear how that statement contributed to the security of the system storing the scanned drivers licence information.

Procedural fairness, which in turn supports transparency, is part of the conceptual framework for assessing the use by the Commissioner of its powers as discussed in Chapter 2. In the absence of other information about the investigation process, the only aspects of procedural fairness which can be assessed by reference to the case notes are the evidentiary basis for the decision, as referred to in the case notes, and the provision of reasons (which has been touched on above).

As discussed in Chapter 2.6.1.3, there must be sufficiently probative evidence to support the findings of fact which are necessary for a decision.[676] Findings must be 'based on evidence that is relevant and logically capable of supporting the findings.'[677] The *Complaints Manual* does not provide detailed guidance as to how to identify or collect relevant evidence, although it does refer to different types of evidence that might be available including copies of audit trails from computer

---

675 Ibid.

676 *ARC Evidence Guide*, above n 238, 1.

677 Ibid 3.

systems and 'corroborative evidence from third parties, often by way of a statutory declaration.'[678]

In identifying the security measures in place in each of the cases, it seems that reliance is placed almost entirely on the evidence provided by the respondents. For example, in describing the clinic's security practices, the case note in *D v Health Service Provider* states that "the clinic advised the Commissioner that all patient files are kept in a lockable cabinet and only the doctor and clinic staff have access to this cabinet." There is no reference to the evidence from the clinic being independently tested or verified. Even in cases which involved more complex information technology systems, there is no indication that independent or expert evidence was sought. For example, in *N v Utility Provider*[679] there is no suggestion that any independent expert testimony was sought to support the Commissioner's view that an access audit trail should be part of the respondent's billing system. However, the ultimate conciliation of the case (with the respondent agreeing to implement a password security system as an interim solution) meant that no final decision on the absence of the audit trail needed to be made. Even in those cases where the respondent is found to have breached NPP 4, there is no indication of the Commissioner seeking evidence from a party other than the complainant or the respondent to support that finding.[680]

The failure to seek any corroborating or expert evidence to support assertions made by either party in any of the 23 cases or by the respondents in the OMIs indicates that decisions may be being made that are not based on sufficient evidence. This reliance on evidence provided by the respondent raised issues of procedural fairness (and thus transparency) as well as vigour (as to the collection of relevant evidence) with those reports that have considered NPP 4.

The other finding of note in regard to the evidence relied on are those OMIs reports where reliance was made on evidence of the post-breach remediation steps to

---

678 *Complaints Manual* above n 227, 17.

679 *N v Utility Provider* [2006] PrvCmrA 13.

680 See, eg, *Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16.

determine that there was no breach (as discussed in Chapter 6.4.1). This reliance on post event behaviour is not consistent with reliance on relevant and probative evidence that should be an important part of the process of procedural fairness which should underpin any investigation. It suggests that the Commissioner is more concerned in some of these cases to demonstrate the remediation of any issue, rather than making a finding as to whether or not there has been a breach. This is certainly consistent with the Commissioner's focus on conciliation and with the principles of a responsive regulatory system discussed in Chapter 2. However, the publication of OMI reports where post incident rectification steps are taken into account in determining whether there had been a breach of NPP 4 can be confusing and perhaps misleading. Is the Commissioner's position that organisations will not be found to have breached the NPP 4 if they take appropriate post event remediation steps. This cannot be the intent of these reports.

In summary, the following conclusions can be drawn based on the above:

- Only a small number of cases included statements of general principle in regard to the Commissioner's interpretation of NPP 4 that were consistent with an industry practice approach. There were also few indications of the actual application of an industry practice approach in the Commissioner's consideration of whether or not there has been a breach of NPP 4 in the relevant cases;
- There were few consistent references to the sort of contextual factors which may be expected to influence the determination of what is reasonable (using either an industry practice approach or referring to published guidance from the Commissioner), such as the sensitivity of the information, the size of the organisation or the amount of personal information held. This again indicates an inconsistency with industry practice;
- Although a number of cases arrive at similar conclusions, for example that access controls should have been in place, the failure to properly contextualise those conclusions in the different circumstances make it difficult to derive more than a very general view in regard to the need for individual security measures (such as access controls, logging, physical security, records management systems and appropriate training). This in turn

limits the transparency of decision-making, and the educative value of the reports ;

- There is no indication of the OAIC making independent enquiries or receiving corroborating evidence as to the accuracy of the information provided by the parties in any of the cases. This in turn suggests both a lack of vigour by the OAIC in the investigation process and a failure of transparency to the extent that it is based on procedural fairness and ensuring that decisions are based on appropriate evidence; and
- The findings in a number of the OMI reports are in fact problematic in the way they consider post incident remediation actions as part of whether the respondent organisation has taken reasonable steps.

## 6.5 CONCLUSION

The OAIC's use of the guidance power, through the issuing of guidance documents and the publication of reports on completed investigations, has been considered in this chapter. Although there is some evidence of the more vigorous publication of guidance, including a new *Guide to Information Security*, and greater transparency offered by the extensive range of resources available on-line, ranging from fact sheets to more detailed guides, the overall use of the guidance power in regard to NPP 4 is not entirely consistent with industry practice nor could that use be described as transparent, balance and vigorous.

Prior to 2013, the only guidance that was available in regard to NPP 4 was high level, dealing somewhat generically with the types of controls that should be in place, incomplete and out of date. It was also inconsistent with an industry practice approach, failing to use risk assessment and a process-based approach to information security management to frame the selection and management of the controls. The *Guide to Information Security* issued in April 2013 does not entirely address these issues. Although containing more current detail in regard to the sorts of controls that should be considered, the guidance remains high level, does not include some important controls and still does not provide any overarching framework for the selection and management of security controls. However, this *Guide* is still the only guidance issued by the OAIC specifically relating to information security. In comparison to the wide range of materials available regarding credit reporting and e-

health, for example, it could be said that the use of the power to issue non-binding guidance in regard to NPP 4 has not been balanced or vigorous. The consultation process that preceded the issuing of that Guide suggests that references made in 2008 to the Commissioner's track record of issuing 'vague and ambiguous' guidelines and failure to engage in a well-resourced and properly conducted consultation process as part of the development of guidelines remain pertinent.[681]

In addition to guidance documents, the case notes and pre-February 2011 OMI reports which have considered NPP 4 were assessed using the twin lenses of an industry practice approach to information security and the transparent, balanced and vigorous use of powers. Conclusions similar to those reached in regard to the guidance documents were reached in regard to these reports.

Generally, although there has been an increase in the transparency of this guidance by the publication of more detailed case notes and OMI reports on the OAIC's website, the majority of those case notes and reports fail to align their consideration of NPP 4 with industry best practice. There is limited consideration of risk or even the contextual factors referred to in relevant guidance as being relevant to the assessment of what is "reasonable." With a couple of exceptions, the reports also fail to provide transparency of decision-making or anything more than high level guidance as to the Commissioner's interpretation or application of NPP 4. It also appears that the investigations undertaken may not be sufficiently vigorous to the extent that they seem to rely on evidence provided by the respondents without independent verification and rely on post incident behaviour when determining whether or not there has been a breach.

The findings in this chapter are consistent with those from Chapter 5, which considered the Commissioner's use of its monitoring, audit, advice and education powers.

Accordingly, it can be concluded overall that the Commissioner's oversight powers considered in this Part 2 have not been exercised in a transparent, balanced

---

681 Greenleaf, Waters and Bygrave, above n 65.

and vigorous way or in a way which is entirely consistent with an industry practice approach to information security.

This chapter has considered only those OMI reports issued prior to February 2011, as part of the consideration of the Commissioner's use of its guidance powers, which in turn is one aspect of the Commissioner's use of its oversight powers. The way that the investigation power has been used in regard to data breach cases from 2011 is considered separately in the next Part of this research, which examines more closely the Commissioner's use of its investigation powers through the detailed analysis of six different Own Motion Investigations.

# PART 3: INVESTIGATION POWERS

# Chapter 7: Investigation Powers

In addition to the oversight powers examined in Part 2, the Commissioner has powers of enforcement, referred to as investigation powers in this research because of the Commissioner's focus on the use of the investigation power. The Commissioner's enforcement powers are closer to the more traditional deterrent powers and prior to March 2014 comprised:

- The right to investigate complaints and other interferences with privacy;[682] and
- The power to make a determination following a complaint-based investigation.[683]

In addition, the Commissioner has the power to seek an injunction to prevent conduct that would constitute a breach of the Act.[684] Because this power has not been exercised by the Commissioner, it will not be considered in this research.

Additional powers have been made available to the Commissioner but because these came into effect in March 2014, they will not be considered in detail in this research.[685]

The ALRC referred to the importance of the enforcement functions of the Commissioner. The ALRC noted Julia Black's statement that enforcement can play a pivotal role in providing 'incentive structures' to promote compliance, although

---

682 *Privacy Act*, s 40.

683 Ibid s52.

684 *Privacy Act* s 98. Section 98 provides that following an application from the Commissioner or another person, the Federal Court or Federal Magistrates Court can grant an injunction restraining a person from engaging in conduct that would constitute a contravention of the *Privacy Act* and, if the court thinks it desirable to do so, requiring a person to do any act or thing.

685 The Commissioner's new powers are considered briefly in Chapters 2.4 and 11.

initial focus should be on restoring compliance through negotiated outcomes (such as conciliation).[686]

This Part 3 will consider and analyse these enforcement powers by reference to the 6 investigations conducted by the OAIC introduced in Chapter 4. Each of these investigations will be assessed using the conceptual framework of standard information security practice and principles for the exercise of regulatory powers, developed in Part 1. Part 3 is made up of the following chapters: Chapter 7, which provides an overview of the Commissioner's investigation powers and the guidance that the Commissioner has issued in regard to the use of those powers; Chapter 8, in which the 6 investigations that are considered in detail in this research are introduced; Chapter 9, which considers the extent to which the investigation in each of the 6 cases represents the transparent, balanced and vigorous use by the Commissioner of its investigation power and Chapter 10, which considers the extent to which each of the investigations could be regarded as supporting an industry practice approach to information security.

## 7.1 INVESTIGATION FUNCTIONS

The *Privacy Act* provides a process for individuals to complain to the Commissioner about acts or practices that may be an interference with individuals' privacy rights,[687] which are defined to include, among other things, a breach of the privacy principles.[688] The Commissioner generally is required to investigate if a complaint had been made,[689] although there were some exceptions to this[690] and the Commissioner has the discretion to decide not to investigate, or to cease an investigation, in certain circumstances.[691]

---

686 *For your information,* above n 32, [4.72].

687 *Privacy Act* s 36.

688 Ibid ss 13, 13A.

689 Ibid s 40.

690 Ibid s 40(1A), eg, if the complainant did not complain to the entity first.

691 Ibid ss 41(1), (2) & (3).

The Commissioner also has the discretion to investigate an act or practice that may be an interference with an individual's privacy even if there is no complaint, if the Commissioner thinks it is desirable that the act or practice be investigated.[692] For example, if the media reports a serious breach of privacy, the Privacy Commissioner may take action and investigate before a complaint is made.[693] These investigations were reported as 'Own Motion Investigations'[694] and in this chapter are considered separately to complaint-based investigations.

### 7.1.1 Conducting investigations

In terms of the investigatory process, the Act provides that the Commissioner must inform the respondent that the matter is to be investigated before commencing the investigation[695] but is not required to provide either the complainant or the respondent with an opportunity to appear before it unless it proposes to make an adverse determination pursuant to Section 52.[696] The Act also specifies that the investigation shall be conducted in private 'but otherwise in such manner as the Commissioner thinks fit.'[697] Accordingly, the Commissioner can determine the process that will be used for investigations and may, for example, make decisions based on a review of relevant documentation without any hearing in person.[698]

The OAIC has issued guidance as to how its investigations will be handled.[699] This guidance provides in summary that:

---

692 Ibid s 40(2).

693 Office of the Australian Information Commissioner, *Applying Privacy Law* (1 September 2014) < http://www.oaic.gov.au/privacy/privacy-act/applying-privacy-law>.

694 From 12 March 2014, these investigations will be referred to as Commissioner Initiated Investigations. See Office of the Australian Information Commissioner,*Commissioner initiated investigation reports* (30 June 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

695 *Privacy Act* s 43(1)(a).

696 Ibid ss 43(4) - (5).

697 Ibid s 43(2).

698 This is consistent with the general law which provides that if the relevant legislation does not prescribe how the investigation should be conducted, then the regulator may decide on what is appropriate. See, eg,, *Kawicki v Legal Services Commissioner and Anor* [2002] NSWSC 1072

699 *Fact Sheet 11*, above n 596.

- A Compliance Officer, who has authority to make decisions about complaints on behalf of the Commissioner, will investigate;
- The Compliance Officer will contact the complainant to discuss the complaint and ask what they are seeking for resolution and will also contact the organisation responsible;
- The Compliance Officer will also ask for parties to provide evidence to support their views;
- If there is enough evidence to support the complaint, the Compliance Officer will try to resolve it through conciliation, and if successful, the file will be closed;
- If the OAIC is of the view that the respondent has made a reasonable offer but the complainant has not accepted it, the OAIC can close the file on the grounds that the respondent has adequately dealt with the matter; and
- If the OAIC does not think the respondent has taken reasonable steps to deal with the matter, the Commissioner can make a formal decision or determination, which may include orders for the respondent to apologise, pay compensation or change its practices.[700]

As previously discussed, in addition to this general guidance, the Commissioner has also published a *Complaints Manual,* which provides more detailed information about the OAIC's investigation process. According to the *Complaints Manual*, the OAIC must undertake a number of preliminary steps to ensure the complaint is one that should be investigated.[701] One of those is an initial complaint assessment.[702] If that assessment results in a decision to proceed with the investigation, the next steps are:

---

700 Ibid.

701 *Complaints Manual* above n 226, 13.

702 The complaint assessment process is considered in more detail by reference to the Complaint Assessment Sheets discussed in Chapter 9.4.

- Preparing a case plan that includes identification of the issues in the complaint and the appropriate areas of the Act that may be relevant;
- Sending a letter advising the parties about the investigation (referred to in this research as the Request for Information Letters or RFI Letters);
- Collecting relevant evidence to apply the law and relevant policy to the facts of the case; and
- Finalising the case, which will occur by conciliation or by closing the case on the grounds that there has been no interference with privacy or by making a determination.[703]

The *Manual* provides that a case plan for each investigation should be drafted using a template within the Complaint Management System (CMS). The case plan should identify the issues raised by the complaint, the relevant privacy principles that may have been breached and the information or evidence needed to establish whether there has been a breach of privacy. In determining what information or evidence may be required, the *Complaints Manual* provides that consideration should be given to any evidence to hand in relation to the allegations, identifying what information or evidence is still needed.[704] These case plans must be approved by the Complaint Officer's supervisor before investigation-opening letters are sent.[705]

Case plans or investigation plans are an important part of any investigation. For example, the Commonwealth Ombudsman's investigation guide refers to the creation of such a plan and notes the benefits, which include that the plan focuses attention on what is to be investigated. This will ensure that important matters are not overlooked and that the investigation does not wander off course. [706] Plans also support transparency of the investigation process and play an important role in

---

703 *Complaints Manual* above n 226, Section 12.

704 *Complaints Manual* above n 226, 33.

705 Ibid.

706 Commonwealth Ombudsman, 'Better Practice Guide to Complaint Handling', (April 2009) < http://www.ombudsman.gov.au/docs/better-practice-guides/onlineBetterPracticeGuide.pdf>, [4.23].

identifying the evidence that is needed to form a decision regarding the issues raised by the complaint. The extent to which the OAIC follows this process is considered in Chapter 9.

Although the Compliance Officers are largely responsible for the carriage of the investigations, there is no indication of what the investigative skills or background of those officers should be. The *Complaints Manual* states that Compliance Officers will 'provide excellent service to people making or responding to complaints.'[707] It also states that Compliance Officers should be continually developing understanding and expertise in privacy issues and the Act.[708] However, there is no reference to the need for Compliance Officers to have any specific investigative skills or experience. When the question of investigation skills was raised with the ACC, who has a legal background, she advised that 'in terms of formal investigative qualifications I am aware that there are specific qualifications for investigations and we've certainly put some of our people through that kind of training.'[709] However, there is no reference to any particular investigation training or similar skills of the OAIC staff in any of the OAIC's annual reports or other publications. The OAIC *2013 Annual Report* refers to staff training that took place, including external courses on leadership and staff management, media, social media, strategic communications, speech writing and project management, as well as internal learning and development opportunities.[710] There is no reference to training or development regarding investigation skills or information security.

The skills of the regulatory team are important. As noted in Chapter 2.5, principle- based regulation shifts responsibility for determining how to comply from the regulator to the regulated entities, which requires a substantially different set of skills on the part of inspectors and compliance staff to enable them to engage in the negotiations and qualitative judgement that are entailed.[711] Lack of skills, whether

---

707 *Complaints Manual* above n 226 at 6.

708 Ibid.

709 Interview with Acting Commissioner Compliance (Sydney, 14 December 2012).

710 *OAIC 2013 Annual Report,* above n 381, 22.

711 Black, above n 179.

in investigation techniques or in understanding information security practice, are likely to affect the Commissioner's use of its investigation and enforcement functions. This is even more so in relation to cases which involve complex technical issues.

### 7.1.2 Conciliation

If the investigation is not closed earlier for other reasons, the Commissioner can endeavour, by conciliation, to effect a settlement between the complainant and respondent of the matters that gave rise to the investigation.[712] The Commissioner can also make a determination either dismissing the complaint or finding the complaint substantiated.[713]

The OAIC is focused on conciliation.[714] It sees conciliation as an 'effective and quick way both parties can reach an agreement.'[715] The proposed *Regulatory Powers Policy* confirms this preference for conciliation. It provides that, in response to a complaint, the OAIC will investigate and attempt to conciliate and only 'if satisfied that there is no reasonable likelihood that the complaint will be resolved by conciliation' will the OAIC decide whether to investigate the matter further and perhaps make a determination.[716] Although the OAIC has stated that there are cases, such as 'particularly serious privacy breaches,' where the OAIC would be prepared to use its power to make determinations rather than rely on conciliation, to date the

---

712 *Privacy Act* ss 27(1)(a), 27(1)(ab).

713 Ibid s 52.

714 See, eg, 'Communication Privacy Complaints: In Search of the Right Path', 4; Nigel Waters, 'Enforcement of Privacy Law – Issues Arising from Australian Experience' (2007). See also comments by the Commissioner in C Merritt, 'Pilgrim has compelling case for conciliated outcomes', *The Australian* (online), 19 August 2011 <http://www.theaustralian.com.au/business/legal-affairs/compelling-case-for-conciliated-outcomes/story-e6frg97x-1226117737294> ; A Colley, 'Privacy Commissioner plans hardline approach to new Act. Talks tough on *Privacy Act* amendments', *itNews* (online), 25 November 2013 <http://www.itnews.com.au/News/365375,privacy-commissioner-plans-hardline-approach-to-new-act.aspx>.

715 Ibid.

716 *Regulatory Powers Policy, above n 227* at 6.

determination power seems to have only been used where a conciliated outcome cannot be reached.[717] Determinations are discussed further in Chapter 7.3 below.

Although the *Privacy Act* does not prescribe how the conciliation process is to be conducted, the OPC and the OAIC have released a number of relevant guidance documents.[718] In these, conciliation is defined as 'a formal, structured discussion between the parties assisted by an OAIC conciliator, an independent third party who helps identify and discuss issues.'[719] Information is sought from the complainant about the desired outcome of the complaint and the respondent is then contacted to determine whether it agrees to the complainant's solution, or the parties are brought together in a conciliation conference. If the parties reach an agreement during conciliation, the OAIC regards the case as settled. The OAIC's view is that has been very successful in the use of its power to achieve conciliation, which is one of the reasons that so few determinations have been made.[720]

The OAIC's preference for conciliated outcomes is entirely consistent with the objects of the Act in relation to the investigation of complaints. However, it is not clear that the same preference should apply to own motion investigations (which do not involve a complainant and do not have the same legislative direction to conciliation). It is also not clear that conciliation is appropriate where systemic issues are raised. These issues are discussed further below.

### 7.1.3 Closing a complaint investigation

There are circumstances in which the Commissioner may decide to close an investigation without arriving at a conciliated outcome or making a determination.

---

717 Timothy Pilgrim, 'Privacy What's Ahead for 2012' (Presentation to International Association of Privacy Professionals Australia & New Zealand, Annual Summit, 30 November 2011).

718 Guidance includes Office of the Australian Information Commissioner, 'About the Office Information Sheet – Conciliation of Privacy Complaints' (February 2008).

719 Office of the Australian Information Commissioner, 'Privacy fact sheet 12: Conciliation of privacy complaints', (June 2012) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-12-conciliation-of-privacy-complaints>.

720 In the Senate Committee Review of the recent *Privacy Act* amendments, the Commissioner argued that the low number of determinations reflected the Commissioner's success in conciliating matters rather than the Commissioner having to use more formal powers. See Senate Report 2012, [5.12].

One of those circumstances is that there has been no interference with privacy.[721] In the last reporting year, 55% of complaints were closed without a complete investigation.[722] The other common basis for closing complaint-based investigations is that the Commissioner believes that the interference complained of has been adequately dealt with.[723] In the 2012–2013 year, 83 of the 153 cases that proceeded to an investigation were closed on this basis.[724] The *Complaints Manual* refers to the different ways that the OAIC may be satisfied that the respondent has addressed the complainant's concerns, including where the respondent:

- Apologised;
- Instituted systemic reform of its processes and procedures;
- Provided training;
- Reinforced or strengthened security measures for personal information; or
- Offered appropriate compensation to the complainant.[725]

This list is consistent with that provided as the grounds for closing complaints on the basis that they had been adequately dealt with in the OAIC's last *Annual Report.*[726]

Before leaving consideration of instances where investigations are closed without a determination, it is worth noting that this decision (to cease the investigation) is subject to judicial review by the Federal Court under the *Administrative Decisions (Judicial Review) Act 1977* (the 'ADJR Act'). Judicial review is not a merits review. It is limited to a consideration of the legality of the process, including issues such as a breach of natural justice; error of law; and an improper exercise of power. The court cannot hear the matter afresh or substitute the

---

721 *Privacy Act* s 41(1)(a).

722 See, eg, *OAIC 2013 Annual Report*, above n 381, 71. For a discussion on the effect of closing investigations based on there being no interference with privacy – see Waters, above n 65.

723 *Privacy Act* s 41(2)(a).

724 *OAIC 2013 Annual Report*, above n 381, 75

725 *Complaints Manual*, above n 227, 'Section 41(2)(a) – adequately dealt with.'

726 *OAIC 2013 Annual Report,* above n 381, 76.

decision of the Commissioner with its own. If the court finds that the grounds for review are made out, it can make an order setting aside or quashing the decision and can remit the matter back to the Privacy Commissioner for further reconsideration.[727] From a practical point of view, the judicial review process is expensive (because it involves applying to a court, with all the attendant filing and legal representation costs) and time consuming. To date, most applications for review have been dismissed without consideration of the privacy principles.[728] In only two cases has the Court considered the Commissioner's interpretation of the privacy principles as part of its decision regarding whether there has been a mistake in law.[729] Neither of those cases involved consideration of NPP 4.

There is no right to a merits review of any decision to cease an investigation. This has not changed with the amendments, which introduce a right of appeal on the facts only in regard to determinations.[730] The absence of this right has contributed to the lack of jurisprudence around privacy law in Australia.[731] One of the consequences of this lack of jurisprudence is the increased importance of the Commissioner's case notes and OMI reports, because they are one of the few resources available that provide insight into the Commissioner's interpretation and application of the privacy principles.

### 7.1.4 Publishing case notes

The OAIC aims to publish a number of case notes each year.[732] The nature and format of case notes and OMI reports has been discussed.[733] The role of case notes

---

727 *For your information,* above n 32, [46.49] – [46.41].

728 See, eg, *A v Australian Information Commissioner* [2011] FCA 520; *Wijayaweera v Australian Information Commissioner* [2012] FCA 99; *Hammond v Australian Information Commissioner* [2013] FCA 802.

729 *Smallbone v NSW Bar Association* [2011] FCA 1145; *Jones v Office of the Australian Information Commissioner* [2014] FCA 285. The privacy principles were considered by the Federal Court in *Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637; but in the context of the issuing of injunctive relief pursuant to old s 98.

730 *Privacy Act* s 96(1)(c).

731 See Chapter 7.1.4.

732 *Guide to Producing Case Notes,* above n 248, 1.

733 See Chapter 6.4.

and OMI reports as guidance, and the extent to which case notes and OMI reports published prior to February 2011 provide transparency of decision-making and represent the vigorous use of the Commissioner's powers, has also been discussed.[734]

In addition to transparency of decision-making, two other reasons are given for the publication of case notes and OMI reports: transparency of compliance activities and deterrence. The *OAIC 2012 Annual Report* refers to the Privacy Commissioner commencing the publication of reports on investigations into high-profile cases to 'increase the transparency of its compliance activities.'[735] A similar statement is included in the *OAIC 2013 Annual Report*.[736] The draft Regulatory Powers Policy refers to public communication about regulatory activity, calling it an important tool for the OAIC because it may promote community confidence in the OAIC by clearly signalling the way that the OAIC intends to deal with entities that are not complying with privacy laws, and because it will support transparency around the OAIC's use of privacy regulatory powers. [737] The concern to ensure transparency of compliance activities is also consistent with at least one of the criterion for opening an OMI: that there is a general public expectation that the OAIC will investigate breaches of the Act. If the OAIC takes action on this basis, then it is important that the community generally is aware of the action taken. Given that the Commissioner has been criticised for its failure to take action[738] it is perhaps not surprising that one of the motivations for the publication of reports is to provide greater transparency and promote awareness of its compliance activity.

This interest in the public communication of regulatory activity indicates a significant shift by the OAIC. The Commissioner's previous approach to promoting compliance noted that details of investigations may be published in 'rare circumstances where this may be of merit' such as repeated or very serious breaches or where the organisation demonstrates that it does not intend to comply with its

---

734 Ibid.

735 *OAIC 2012 Annual Report*, above n 1, 64.

736 *OAIC 2013 Annual Report,* above n 381, 78.

737 *Regulatory Powers Policy, above n 227*, [49] – [50].

738 See the references above n 65.

legal obligations.[739] This reflects the previous position that details of an investigation, particularly the respondent's name, may have been published for deterrent purposes (albeit rarely) rather than more generally as part of supporting compliance.

The deterrence value of the publication of details of the Commissioner's investigations is no longer clear.[740] The *Complaints Manual* notes that details of investigations may be published in 'rare circumstances where this may be of merit,' such as where there has been publicity around the matter before it comes to the Office, or repeated or very serious breaches or where the organisation demonstrates that it does not intend to comply with its legal obligations.[741] Presumably the assumption is that organisations do not want to run the risk of reputational damage and loss of clients' trust from published reports of privacy breaches, particularly if these are critical of the respondent organisation (unless the case is already in the public domain). For this reason, prior to February 2011 most OMI reports were published on an anonymous basis, for example *OMI v Airline Company*.[742] More recently however, the media coverage of data breaches means that the incidents are often already in the public domain before the Commissioner decides to undertake any investigation. In many cases, the media, as part of its reporting on the data breach, will approach the Commissioner for a public statement regarding whether the Commissioner intends to conduct an investigation.[743] In these circumstances, where the data breach and the entities involved are already in the public domain, the publication of details of the OAIC's investigation, including the name of the respondent organisation, would no longer seem to be any sort of deterrent. In fact, as

---

739 *Information Sheet 13*, above n 203, 2.

740 *OAIC 2012 Annual Report,* above n 1, 38; *Information Sheet 13*, above n 203, 2.

741 *Complaints Manual*, above n 227, 2.

742 *Own Motion Investigation v Airline* [2009] PrivCmrA 7.

743 See, eg, Fran Foo, 'Warning after eBay passwords "stolen"', *The Australian* (online), 23 May 2014 <http://www.theaustralian.com.au/technology/warning-after-ebay-passwords-stolen/story-e6frgakx-1226927542280>, which includes the following statement: 'Australia's Privacy Commissioner Timothy Pilgrim said the Office of the Australian Information Commissioner had received a voluntary data breach notification from eBay early yesterday. "We are currently conducting enquiries into the data breach to inform whether the OAIC will need to open an investigation," Mr Pilgrim said.'

discussed in Chapter 9, the Commissioner has argued that publication is of benefit to the respondent, giving it the opportunity to reassure the community that the issue has been resolved.[744]

The extent to which these different purposes for the publication of reports - transparency of decision-making , transparency of compliance activities and deterrence – are met by the reports published in regard to the 6 investigations analysed in detailed in this research is considered further in Chapter 9.

### 7.1.5 Procedure for producing case notes

The OAIC's *Guide to Producing Case Notes* provides a process for the selection of cases from which to publish a case note. The process involves a case officer flagging potential cases for publication of case notes. These are then given further consideration by the case note Project Manager, who then consults the OAIC Compliance Directors where appropriate.[745] The Compliance Directors review the drafts with regard to content, style and suitability for publication. Once approved, the drafts are sent to the Director of Corporate and Public Affairs for style checking before being sent to the Commissioner, Assistant Commissioner, and Deputy Commissioner for their consideration. Following clearance by the Executive, the case note is published.[746]

It is difficult to determine from the published case notes themselves whether the approval process set out in the Guide has been followed generally. However, the selection of OMIs for reporting will be considered in more detail in Chapter 9 of this research, where additional information from the OAIC's investigation files is available to support that analysis.

## 7.2 OWN MOTION INVESTIGATIONS

As already mentioned, the Privacy Commissioner has the power to investigate possible non-compliance with the Act on its own motion, without any complaint

---

744 See Chapter 9.10.

745 *Guide to Producing Case Notes,* above n 248, 3.

746 Ibid 8.

being made. These investigations have been called own motion investigations (or OMIs). From March 2014 they will be known as 'Commissioner Initiated Investigations' or CIIs[747]

### 7.2.1 Commencing an OMI

According to the OAIC, matters that are considered for own motion investigation come to the OAIC's attention in a variety of ways, including reports in the media and from other agencies and organisations, calls to the telephone Enquiries Line or letters to the OAIC from individuals regarding experiences of other people. Also, individuals might complain about something that happened to them, but do not want to make a formal complaint about the practice.[748] There are also cases where entities 'self-report' breaches as part of voluntary data breach notification.[749]

When determining whether to investigate a matter on its own motion, the OAIC uses its own risk assessment criteria.[750] These criteria include:

- The number of people affected and the possible consequences for those individuals;
- The sensitivity of the personal information involved;
- The progress of an agency's or organisation's own investigation into the matter and consideration of the actions taken by the entity in response;
- The likelihood that the investigation will reveal acts or practices that involve systemic interferences with privacy and/or that are unidentified;
- The expertise and resources available to the OAIC;
- The necessity for the OAIC to be satisfied that the investigation is complete and/or proposed resolutions are implemented;

---

747 *OAIC 2013 Annual Report*, above n 381, 77.

748 *Complaints* Manual, above n 227, 20.

749 Both Sony and Dell reported the data breaches which led to the investigations considered in more detail in the subsequent chapters of this research.

750 See, eg, *OAIC 2013 Annual Report,* above n 381, 77; *OAIC 2012 Annual Report*, above n 1, 67 – 68.

- The nature of any proposed resolution; and
- The general public and parliamentary expectations that if it becomes aware of a breach, the OAIC will investigate where appropriate.[751]

The OAIC's reference to these criteria was confirmed by the Assistant Commissioner Compliance. The Assistant Commissioner Compliance said that, rather than investigate where there is one individual who has been affected by a matter, the OAIC's preference is to 'open investigations where there's systemic problems, large numbers of people affected, or the information that might have been say revealed may have been particularly sensitive.'[752] According to the Assistant Commissioner Compliance, these criteria were used for resource reasons, because the OAIC does not have the capacity to investigate every report of possible breach.[753]

The extent to which these criteria have been used as the basis for the commencement of OMIs is considered in Chapter 9.

### 7.2.2 Conducting an OMI

According to the *Complaints Manual*, the Commissioner will take the same approach to own motion investigations as it does to complaint-based investigations.[754] This investigation process has already been discussed in Chapter 7.1 and will be assumed to apply to OMIs.

However, some differences in the investigatory process between compliant-based and own motion investigations might be expected. The *Complaints Manual* refers to the problems for case officers inherent in the differing roles of investigator and conciliator, observing that: 'In some ways these roles are complementary but in other ways there is a tension as their ultimate goals may be different.'[755] It describes

---

751 See, eg, *Getting in on the Act*, above n 155, 355; *OAIC 2013 Annual Report,* above n 381, 77, *OAIC 2012 Annual Report*, above n 1, 67 – 68; *Complaints Manual*, above n 227, 'Current criteria for conducting own motion investigations'.

752 Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

753 Ibid.

754 *Information Sheet 13*, above n 203.

755 *Complaints Manual*, above n 227, 'Case Officer's Role', 7.

the investigation function as aiming 'to come to a view about whether a privacy breach has occurred or not.' It notes that, although still needing to adhere to principles of procedural fairness, the role of investigator is not one that takes into account the particular needs or interests of the parties.[756] It then contrasts the conciliation function, where the complaint officer is concerned with the interests of the parties and how they might be met by a conciliated outcome. Where the focus is on conciliation, the OAIC officer:

> is not gathering information for the purpose of forming a view about the facts of the matter or whether the law has been breached. A view regarding the facts of the matter may remain suspended whilst the parties focus on a solution they can both accept.[757]

Having described this fundamental difference between an investigation and a conciliated outcome, the *Manual* fails to incorporate this into any meaningful differentiation in its approach to the conduct of own motion investigations.

If OMIs are pursued with a view to reaching agreement with the respondents, this may impact the manner of the investigation and may take precedence over the OAIC's concern to form a view about the facts of each matter or about whether the law has been breached, having regard to those findings of fact. This is of particular relevance to the investigation of those data breach cases that raise systemic issues. It would be expected that the report from an investigation into a systemic issue would identify an issue of general concern and clearly describe how the *Privacy Act* principles would apply, rather than seek to arrive at a 'conciliated' or agreed outcome with the organisation.

Another aspect of an interest in resolving OMIs by agreement is the OAIC's relationship with respondents. It is clear that the OAIC is concerned to ensure the continued voluntary cooperation of respondents in own motion investigations. As noted in Chapter 4.3.2, the majority of redactions made as part of the FOI process were on the basis that if the information was revealed it would impact the flow of information to the OAIC. In weighing the public interest in disclosure, the OAIC's

---

[756] Ibid.

[757] Ibid.

concern to ensure the continued voluntary provision of information by respondents was identified as a decisive concern. In the interview with the researcher, the Assistant Commissioner Compliance referred to how cooperative the respondents had been, noting that although the OAIC does have compulsory powers that it could use, the respondents had been 'cooperative and accept the views that we come to in general.'[758] The OAIC's compulsory powers include the power to require the production of documents and for witnesses to give evidence.[759] The effect of the OAIC's interest in maintaining open communications with respondents in OMIs on the transparency and balance of the exercise of its investigations powers will be considered as part of the detailed assessment of the OMI reports contained later in this research.

### 7.2.3 Outcome of OMIs

Prior to the amendments that became effective in March 2014, there was no action that the Commissioner could take based on the outcome of an OMI into a breach of NPP 4: no determination or other order could be made. This was the case even if the OAIC had determined that an egregious and continuing interference with the privacy of Australians was occurring.

When asked by the researcher what outcome the Commissioner had in mind when undertaking an OMI, the Commissioner responded that, if there had been a failing under NPP4, it was looking 'to get the organisation to change its systems or its practices.' The Commissioner also noted that 'in the majority of these cases organisations are obviously going to be willing to do that particularly if the matter has been at the forefront of the media.' The Commissioner referred to the importance of trust to organisations and how, if organisations have failed to properly secure personal information, they need to 'make sure that they're seen to be taking appropriate steps to remedy it and improve their systems and that's what we're looking for.'[760] The Commissioner also referred to the success of the office in

---

758 Interview with Assistant Commissioner Compliance (Syndey 12 December 2012).

759 *Privacy Act*, s 40.

760 Interview with Timothy Pilgrim (Sydney, 14 December 2012).

reaching agreement with entities regarding the steps to be taken to fix breaches. The Assistant Commissioner Compliance made a similar statement in regard to the approach to OMIs, saying that the OAIC seeks to arrive at agreed findings and agreed remediation steps to address a breach. The OAIC's stated approach to OMIs supports this focus on remediation: the action by the Office 'will depend upon the respondent's acknowledgment of the breach and its preparedness to take appropriate remedial action.'[761]

The tensions between conciliating or reaching an agreement on an outcome and conducting an investigation have been discussed above. Consideration of this tension will also be part of the analysis of the 6 OMIs reported on after February 2011 contained in Chapters 9 and 10.

### 7.2.4 Systemic issues

The OMI has been regarded as an appropriate method to deal with large and complex issues. The *Complaints Manual* provides that the OAIC will use its OMI power to 'strive to identify and address systemic issues.'[762] The investigation can be directed at resolving systemic issues, without necessarily being concerned to address the needs of a complainant. Similarly, the reasons for commencing an OMI include the 'likelihood that the investigation will reveal acts or practices that involve systemic interferences with privacy.'[763] Annual reports refer to the OAIC using its OMI powers as 'important regulatory oversight in relation to individual complaints and systemic issues'[764]

'Systemic issues' are 'issues that are about an organisation's or industry's practice rather than about an isolated incident.'[765] Systemic issues include:

---

761 *Information Sheet 13*, above n 203.

762 *Complaints Manual*, above n 227, 'OAIC's approach to complaint handling'.

763 See Chapter 7.2.

764 See eg, *OPC 2010 Annual Report*, above n 403, 4; which provides that the Commissioner undertakes 'OMIs where it appears that a breach of the *Privacy Act* may have occurred and it is thought to be desirable that an OMI be undertaken. For example ... in circumstances where the alleged breach raises systemic and/ or ongoing issues.'

765 *Getting in on the Act*, above n 155, 130.

- Widespread poor privacy practice at a large company or agency; and
- Widespread breaches of privacy across an industry.[766]

The OPC's ability to deal with systemic issues was considered in 2005, at which time it was noted that the OPC's 'limited focus on systemic issues and its lack of power to deal with systemic issues' was out of step with best practice for complaint handlers.[767] The issues identified with using the OMI power for these purposes included the impact on the OPC's resources and the lack of the Commissioner's power to direct the respondent to address any issues found during the OMI, and then to enforce those directions.[768]

The ALRC also considered the effect of the strain on the available resources caused by the need to consider all complaints on the Commissioner's ability to deal with systemic issues, [769] making various recommendations that have been included in the amended Act.[770]

The Commissioner's interest in identifying and pursuing systemic issues is of particular relevance to information security failures.

Information security cases, particularly those that involve unauthorised access to personal information as a result of attacks by hackers (such as in the Sony PlayStation Network hack[771]), often raise organisational systemic issues. Effective security relies on the proper operation of a complex system of security measures. Most data breaches result from the failure or compromise of more than one control. Accordingly, most enquiries into whether there were 'reasonable' measures in place for the purposes of NPP 4would involve consideration of the information security management system as a whole.

---

766 Ibid. See also *Complaints Manual*, above n 227, 'Grounds for expedited investigations'.

767 *Getting in on the Act*, above n 155, 150.

768 Ibid, 155.

769 See, eg, *For your information,* above n 32, 1650 – 1652, [49-11], Recommendation 49-2.

770 *Privacy Act* s 41.

771 The Sony PlayStation Network hack is discussed in Chapter 8.1.3.

Similarly, information security incidents also often raise issues of industry-wide systemic problems. Many large organisations adopt the same general systems and so are targeted by attackers using the same types of attack, to exploit the same vulnerability. Incidents affecting one organisation, in the context of the systems and practices in place, usually have relevance to other organisations of the same size or in the same industry sector.[772] This can be demonstrated, for example, by the number of cases which deal with the inappropriate disposal of medical records.[773] The recurrence of this issue might be regarded as an industry-wide systemic problem.

The identification and resolution of systemic issues, particularly industry system issues, is a different objective to that of resolving an individual's complaint. Typically, the resolution of a complaint will involve the reconciliation of the interests of the complainant and the entity alleged to have breached the Act.[774] By contrast, the investigation and resolution of systemic issues is directed at ensuring that the entity's systems are remediated, if required, so that similar incidents do not recur, and also towards providing information to the public in the case of industry-wide breaches of privacy. Accordingly, it would be expected that the investigation into whether there were a systemic issue would consider not just the immediate reasons for any breach but would take a broader view of the organisational controls in place because it would be assessing whether there were an organisation-wide failing. It might also be expected that the case report might include more detail about the failure, the reasons why it was regarded as failing to meet the requirements of NPP 4 and what the respondent should do to address the identified failures. If the Commissioner were of the view that the failure was possibly an industry-wide case, then it might be appropriate to use that finding to provide more general education and guidance.

---

772 For example, the OAIC's OMI reports reveal that Telstra and Vodafone (both telecommunication companies) both used Siebel data management software systems to manage customer personal information.

773 See, eg, *Own Motion Investigation v Medical Centre* [2009] PrivCmr 6.

774 The investigation and resolution of complaints pursuant to the *Privacy Act* are discussed in Chapter 7.1.

The extent to which the OMI power has been used to identify and address systemic issues as reflected in published OMI reports will be considered in the analysis included in the following chapters.

### 7.2.5 ALRC Review of Own Motion Investigation Power

As already referred to, one of the issues for the Commissioner prior to March 2014 was the absence of enforcement options where the Commissioner had carried out an own motion investigation. In accordance with its view that OMIs are a valuable tool where allegations come to light via means other than lodgement of a complaint, the ALRC recommended that the Commissioner should have additional powers following an OMI.[775] Although the specific ALRC recommendations were not adopted, the Commissioner has been given the right to make a determination at the conclusion of an own motion investigation in the same manner as if the investigation were based on a complaint.[776]

## 7.3 DETERMINATIONS

Prior to March 2014, the strongest enforcement power of the Commissioner was to make a determination either dismissing a complaint or finding it substantiated.[777] The Commissioner, when making a determination, also had the right to make a declaration that the respondent acted to redress any loss or damage[778] or paid an amount by way of compensation,[779] at least in the case of complaint-based investigations.[780] The ALRC saw a determination as a 'strong' penalty, because it can involve a public declaration of breach and thereby contain an element of

---

775 *For your information,* above n 32, Recommendations 50-1(a) and (c), 1654.

776 *Privacy Act* s 52(1A).

777 Ibid s 52(1).

778 Ibid s 52(1)(b)(ii).

779 Ibid s 52(1)(b)(iii), which loss may include injury to feelings or humiliation, pursuant to Section 40(1A). Section 40(1A) that has been repealed under the *Privacy Amendment Act*.

780 Section 52 applies 'After investigating a complaint' and does not refer to investigations commenced on the Commissioner's own motion pursuant to s 40(2) *Privacy Act*, without there being a complaint.

informal, negative publicity.'[781] This power is one of the compliance options at the top of the Ayres and Braithwaite enforcement pyramid.

However, the Commissioner has to date used its determination power sparingly. Only ten complaint determinations have been made between the commencement of the *Privacy Act* and 30 March 2014. As at March 2014, the most recent privacy breach-related determination had been issued in December 2011.[782] The determination made prior to that was released in April 2004.[783] There is some indication that the Commissioner may be more willing in the future to use its determination power. In February 2012, the Privacy Commissioner said that it would 'not shy away from using my determination powers where it is appropriate to do so.'[784] It recognised the importance of determination to the understanding of the privacy principles, noting that determinations:

> provide a public record of the OAIC's views on how privacy laws should be interpreted, and can assist complainants and respondents to better understand how privacy laws will apply.[785]

Four determinations have been issued since that speech, one relating to a breach of the credit reporting provisions[786] and the other three, all issued after March 2014, in regard to the privacy principles.[787]

This research is limited to detailed consideration of determinations issued prior to March 2014. NPP 4 was referred to in only one determination prior to March 2014

---

781 *For your information,* above n 32, [50.48].

782 *'D' and Wentworthville Leagues Club* [2011] AICmr 9 <http://www.oaic.gov.au/publications/decisions/2011_aicmr9.html>. One determination was made in 2012 which related to the credit reporting provisions of the Act.

783 A full list of Privacy Commissioner Determinations is available at <http://www.austlii.edu.au/au/cases/cth/PrivCmrACD/>.

784 Timothy Pilgrim, above n 251.

785 Ibid.

786 *S v Veda Advantage Information Services and Solutions Ltd* [2012]AICmr 33.

787 The three new determinations are *'CP' v Department of Defence* [2014] AICmr 88 (2 September 2014); *'CM' and Corporation of the Synod of the Diocese of Brisbane* [2014] AICmr 86 (2 September 2014); '*BO' v AeroCare Pty Ltd* [2014] AICmr 32 (8 April 2014).

and even then only in relation to NPP 4.2.[788] In that determination, no detailed consideration was given to the meaning of the principle. Accordingly, the use of the determination power has offered little in terms of supporting the general understanding of the requirement in NPP 4 to take reasonable steps to protect personal information.

There are a number of possible reasons for the low number of determinations made to date. One reason may be the reluctance of the Commissioner to test its interpretation of the privacy principles in the face of the Federal Court's right to conduct a hearing de novo.[789] Section 55 *Privacy Act* requires that organisations must comply with the terms of a determination. However, if they do not, the Commissioner's only recourse is to make an application for an appropriate order to the Federal Court which will undertake a hearing de novo pursuant to Section 52(1)(b) Privacy Act. It has been suggested that this lack of direct enforceability and the Federal Court's powers have made the Commissioner "determinations-averse."[790] As the Commissioner has not yet had to defend or enforce a determination in court, the extent to which the Federal Court may reasonably defer to the Commissioner's interpretation of a principle or otherwise is still not clear.[791] As noted, in those situations where the Federal Court has been asked to review the Commissioner's decisions, to date it has supported the Commissioner. [792]

---

788 NPP 4.2 was considered in *Complaint Determination No 3 of 2004* but only in relation to its application. There was no detailed consideration of the meaning of the principle. NPP 4 could have been considered in '*'D' and Wentworthville Leagues Club* but does not seem to have been raised.

789 O'Connor, above n 65, 15. See also Greenleaf, Graham, 'The 'Tabula Rasa', above n 65.

790 Ibid.

791 Charles Alexander, Elisabeth Koster and Helen Paterson, 'Punitive powers guided by ambiguity: the Australian Federal Privacy Commissioner's new powers in the context of a principles-based privacy regime' (2013) 9(5) Privacy Law Bulletin

792 To date, most applications for review have been dismissed without consideration of the privacy principles, e.g., *A v Australian Information Commissioner* [2011] FCA 520, *Wijayaweera v Australian Information Commissioner* [2012] FCA 99, *Hammond v Australian Information Commissioner* [2013] FCA 802. There have been only two cases where the Court has considered the Commissioner's interpretation of the privacy principles as part of its decision as to whether or not there has been a mistake in law *Smallbone v NSW Bar Association* [2011] FCA 1145, *Jones v Office of the Australian Information Commissioner* [2014] FCA 285.

Another reason for the low number of determinations may be the Commissioner's 'successes in conciliating claims.[793] As previously noted, the Commissioner closes the majority of complaint-based investigations on the basis that the issue had been adequately dealt with (either by reaching a conciliated outcome with the complainant or the Commissioner forming a view that the respondent had adequately dealt with the complaint).[794] All of the 23 complaint-based investigations which have considered NPP 4 were able to be closed on either of those grounds, even in those cases where the Commissioner found there had been an interference with one of the privacy principles. However, it is difficult to assess whether the resolution of these cases in this way has been regarded as a success by the complainants. Complainants who are not happy with the outcome of the investigation of their complaints have little recourse. There is no right of appeal from the decision to cease an investigation. That decision is only reviewable on questions of law, and not on the facts.[795] In those cases where complainants have gone to the Federal Court for review, the Federal Court has elected in most instances either not to review or to support the Commissioner's decisions.[796] Complainants also have no right to require the Commissioner to make a determination. Such a right if available would benefit complainants who disagreed with the Commissioner's decision to cease an investigation. This was an issue considered by the ALRC. [797] A majority of stakeholders who made submissions to the ALRC supported complainants having a right to require the Commissioner to make a determination. One submitted that such a right would increase the number of determinations which would mean that there

---

793 In the Senate Committee Review of the recent *Privacy Act* amendments, the Commissioner argued that the low number of determinations reflected the Commissioner's success in conciliating matters rather than the Commissioner having to use more formal powers. See Senate Report 2012, [5.12].

794 See Section 7.1.1 and 7.1.2 above.

795 See Section 7.1.3. The right to review decisions to cease an investigation were considered by the ALRC in *For your information,* above n 32, [49.63] – [ 49.69]. See also [46.52] which stated that judicial review rights extended to a decision not to investigate and a decision not to make a determination or a failure to give reasons to a person adversely affected by a decision of the Commissioner.

796 See cases referred to in n 792 above.

797 *For your information,* above n 32, [49.48], [49.53] – [49.56], [49.63] – [ 49.69].

was 'at last potential for a solid body of jurisprudence to develop about the interpretation' of the Act.[798] The OPC did not support the inclusion of any such right.[799] After considering the submissions, the ALRC recommended that such a right should be available to both complainants and respondents, at least in cases where conciliation had failed, supporting the view that more determination would 'help address concerns … about the lack of jurisprudence on the *Privacy Act*.'[800] Notwithstanding this recommendation, no right for any party to require that a determination be made was included in the recent amendments to the Privacy Act. In any case, the ALRC did not support a right to require determination where a complaint was dismissed.[801]

There have been some changes to the enforceability and review of determinations as a result of the *Privacy Amendment Act*, but not as many as recommended by the ALRC or as supported by privacy advocates.

The government accepted the ALRC recommendation that there be a right of appeal on the merits from a determination to the Administrative Appeals Tribunal.[802] In accepting the recommendation, the government noted that undertaking this 'enhanced review' would 'assist in promoting transparency and accountability in the Commissioner's decisions.'[803] Complainants now have a right to a merits review (not limited to grounds of procedural fairness or a question of law) and the Tribunal will be able to substitute its decision for the decision of the Commissioner. However, before exercising a right to a merit review, a determination must be made

---

798 Ibid, [49.54].

799 Ibid, [49.53].

800 Ibid, [49.65] and Recommendation 49-5.

801 Ibid, [49.69].

802 *Australian Government First Stage Response to the Australian law Reform Commission Report 108* (Australian Govenrment, October 2009). 94<http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf>. See *Privacy Act* s 96(1)(c).

803 Ibid.

by the Commissioner.[804] As discussed, the decision to cease an investigation and not to make a determination is still not reviewable on the merits.

It is not clear that, having regard to some of the reasons given as to why there are so few determinations, this position will change in the future. The Federal Court will still re-hear any action to enforce a determination, complainants still have no right to appeal on the merits from a decision to cease an investigation and there is no right for complainants to require the Commissioner to make a determination.

The impact of the changes to the Commissioner's enforcement powers is considered further in Chapter 11.

## 7.4 CONCLUSION

The Commissioner's enforcement powers include the right to make a determination and to seek an injunction. However, the main enforcement power used to date has been in the conduct of investigations, both based on a complaint and initiated on the Commissioner's own motion. This chapter has largely focused on the Commissioner's procedures for conducting those investigations. These procedures will be used in the analysis of the 6 own motion investigations contained later in this research.

Consideration was also given to the difference between complaint-based investigations and own motion investigations. It was noted that conciliation and investigation required different approaches by the investigator, potentially giving rise to a tension. This tension between conciliation and investigation was raised again in the context of the Commissioner's intended outcomes from the conduct of OMIs. In terms of those outcomes, the Commissioner indicated an interest in ensuring that the particular issue giving rise to the investigation was resolved (rather than using the investigation to promote a better understanding of the Act or address systemic issues). Consideration was also given to the different evidence that may be produced in investigations that involved adversarial parties versus those that involved a single respondent.

---

804 *Privacy Act* s 96(1)(c).

The expectation that the Commissioner would use OMIs to address systemic issues was noted. It was also noted that, where conducting an OMI to resolve a systemic issue, a less conciliatory and more evidence-focused investigation might be undertaken. It might also be expected that a more detailed report with clear findings of fact supporting the decision would be provided.

Each of these issues in terms of the purpose and procedures for investigations will be considered in more detail as part of the analysis of the 6 own motion investigations and resulting reports as contained in Chapters 9 and 10 of this research. The following chapter provides an introduction to the 6 incidents that gave rise to those investigations, establishing the facts of each case and the investigation outcomes. These 6 cases are then considered in more detail through the application of the 2 lenses of the conceptual frameworks (that is, the transparent, balanced and vigorous use of powers, and consistency with an industry approach to information security) in the succeeding chapters.

# Chapter 8: Own Motion Investigations

The Commissioner's investigation powers, including in particular the power to conduct and report on own motion investigations were discussed in the preceding chapter.

Between February 2011 and April 2013,[805] 8 OMI reports were published. This was a greater number than had been published previously over a similar period. As discussed, these reports represented a new approach to dealing with high-profile data breach cases undertaken by the new Privacy Commissioner, Timothy Pilgrim, who had been appointed in mid-2010.[806]

These reports were very different to the OMI reports which had been issued previously. For the first time, they included the name of the respondent organisation; they were not published on an anonymous basis. These reports were longer, ranging from 1224 words (for the Telstra Mail Out report) to 2438 words in the Sony report. The standard format for these reports included a 'Background' and more recently an 'Overview' section, which sections together provided more context for the cases being considered. The Findings sections also were generally much longer and involved a more detailed analysis of the application of the privacy principles to the relevant case. All except 1 report related to incidents that were in the public domain.[807] Most importantly, all 8reports considered the application of NPP 4 and included a finding in regard to NPP4: either the respondent was found to be in breach, or not to be in breach of NPP 4. Unlike the previous OMI reports, none of these investigations were closed without some finding regarding compliance with NPP 4.

---

805 April 2013 is the date at which the first application was made by the researcher for administrative access to the OAIC's investigation files.

806 See Chapter 6.4.1.

807 The *Professional Services Review Agency OMI report*, above n 340, did not relate to an incident that was in the public domain.

Taken together, this group of OMI reports would be expected to provide the most comprehensive and current guidance regarding the Commissioner's interpretation and application of NPP 4 across a range of different circumstances. The 6 OMIs which will be examined in detail to support the assessment of the Commissioner's use of its investigation powers have been selected from this group of OMI reports.

Details of the 6 OMIs, including an overview of each investigation and the outcome of that investigation as contained in the published OMI report, are provided below. This information forms the background for the analysis of the investigations contained in the succeeding chapters.

### 8.1.1 **Telstra Mail Out**

On 27 October 2011, media reported that the Commissioner and the ACMA would look into an incident involving Telstra.[808] An incorrect mail merge completed as part of a bulk mail-out resulted in 220,000 letters being sent to Telstra customers containing the name, phone number and telephone plan of customers other than the recipients of the letter. The letters were sent to explain upcoming fixed-line price changes.[809] The OMI report noted that the Commissioner opened the case following receipt of a notification letter from Telstra.[810] This notification letter provided details of the mail-out error and Telstra's strategy to 'remediate any customer concerns.'[811] Telstra had earlier reported the incident to the ACMA, which also notified the

---

808 See Asher Moses, 'Telstra botched mail-out exposes 220,000 customers', *The Sydney Morning Herald* (online), 27 October 2012 <http://www.smh.com.au/technology/security/telstra-botched-mailout-exposes-220000-customers-20101027-173du.html#ixzz2hC0Ak7np> and AAP 'Massive Telstra bungle a privacy breach', *News.com.au* (online), 27 October 2010 <http://www.news.com.au/business/massive-telstra-bungle-a-privacy-breach/story-e6frfm1i-1225944346111>.

809 Ibid.

810 *Telstra Mail Out OMI Report*, above n 334.

811 Letter from Helen Lewin, Chief Privacy Officer, Telstra to Timothy Pilgrim, Privacy Commissioner, OAIC, 27 October 2010.

OAIC.[812] The OAIC's file includes a copy of the Telstra response to an ACMA letter of 26 October, 2010.[813]

The Commissioner sent its own letter requesting information about the incident (the Telstra Mail Out RFI Letter) on 28 October 2010.[814] In addition to a series of questions that were specific to the breach,[815] 3 more general questions regarding the incident were raised:

- What steps did Telstra have in place to protect customer information from unauthorised disclosure when conducting mail-outs?
- Were these steps in place at the time of the incident? and
- When did Telstra expect that its data analysis of the incident would be complete?[816]

Telstra was asked to respond by 18 November 2010, which at Telstra's request was extended by the OAIC to 30 November 2010. However, it was not until 8 December 2010 that Telstra responded to the Commissioner, presumably providing a detailed explanation in response to the Telstra Mail Out RFI Letter.[817] This document was redacted in its entirety.[818] There is no evidence of any subsequent activity in relation to the investigation until May 2011. On 16 May 2011, a Close Letter was sent confirming that the OAIC was of the view that there was a breach of

---

812 Letter from Jane van Beelen to Olya Booyar, The Australian Communications and Media Authority, 27 October 2010, which refers to 'your letter of 26 October 2010 … requesting further information about this matter.'

813 Ibid.

814 Letter from Timothy Pilgrim to Ms Helen Lewin, 28 October 2010 ('*Teltra Mail Out RFI Letter*'). A copy of that letter is included in Appendix C

815 For eg, 'Please identify the mailing house responsible for the mail out'; 'Please provide a timeline of the incident'; and 'When does Telstra expect its data analysis of the incident will be complete'.

816 The *Telstra Mail Out RFI Letter*, above n 802, is discussed further in Chapter 9.6.

817 Email from Judith McAlpine, Telstra to Emily McGufficke, OAIC, 8 December 2010.

818 The Schedule to the FOI Decision Letter refers to a 'Letter to Timothy Pilgrim from Helen Lewin dated 7 December 2010 entitled 'Own Motion Investigation – Mail List Incident Telstra Corporation Limited (Telstra) Response to Notice under section 44 of the *Privacy Act*', which document was not disclosed.

NPP 2. However, it also found that there was no breach of NPP 4.1, because this was a one-off human error, and as such 'does not mean that Telstra failed to comply with its obligations under NPP 4.1.' [819]

Telstra contended that it was not in breach, stating that:

- The disclosure of a name and an incorrect address (which was the only information visible from an unopened letter) was not a disclosure of personal information because there was no link between the information about the person (e.g. their name) and the person's identity;
- The actual number of customers likely to have had their information disclosed was probably significantly less than 220,000 after the number of letters with incorrect addresses was added to those that had been returned unopened to Telstra;
- They should have had a right to be heard with respect to the application of the privacy principles; and
- The OAIC should not publish a media release about the incident, including its findings. [820]

In support of its position, Telstra referred the OAIC to the case note *OMI v Direct Marketer*,[821] which related to the disclosure of email addresses in a bulk email 'blast', and where no finding of breach was made.[822] The OAIC rejected Telstra's proposition stating that 'a person's name is personal information and does not have to be linked with other information to fall within the definition of personal information as set out in the Act.'[823]

---

819 Letter from Mark Hummerston to Ms Helen Lewin, 16 May 2011 ('*Telstra Mail Out Close Letter*'). A copy of that letter is included in Appendix C.

820 Email from Helen Lewin, Telstra to Timothy Pilgrim, 26 May 2011. A copy of that email is included in Appendix C . A further email repeating these contentions was sent from Helen Lewin, Telstra to Linda King, OAIC, 2 June 2011.

821 *OMI v Direct Marketer* [2008] PrivCmrA 23.

822 Ibid.

823 Email from Linda King, OAIC to Helen Lewin, Telstra, 28 June 2011.

It would seem that a draft of the OMI report was attached to that same email of 28 June 2011.[824] However, no draft or final copy of the OMI report was included in, or referred to, in the list of records provided in response to the FOI request. There is no other record indicating Telstra's response to the terms of the proposed OMI report or any further correspondence on the file.

The final OMI report is one of the shortest, totalling just over three pages and with a format similar to that of earlier OMI reports. It reflects the OAIC's position in the Close Letter finding that there had been an unauthorised disclosure under NPP 2 but no failure to take reasonable steps pursuant to NPP 4 because the incident was the result of a one-off human error.

### 8.1.2 Vodafone Hutchinson Australia Limited

Media reports appeared on 9 January 2011 suggesting that personal details of millions of Vodafone Hutchinson Australia Limited (Vodafone) customers were available on the web and 'criminal groups have paid for the private details of some Vodafone customers in order to blackmail them.'[825] Alleged details that were available included names, home addresses, drivers' licence numbers and credit card details. However, the Commissioner's investigation found that the incident actually involved Vodafone franchisees who could access details of other franchisees' customers, which were all held in an internal Vodafone database. The information was not part of a public website as had been reported.[826]

The incident aroused significant media interest, including a poll by a metropolitan newspaper asking whether the Privacy Commissioner should investigate.[827] In response to these media reports, the Privacy Commissioner

---

824 The email header notes an attachment called '2011_06 TELSTRA c14509 Investigation Report FINAL.docx'.

825 Natalie O'Brien, 'Mobile security outrage: private details accessible on net', *The Sydney Morning Herald* (online), 9 January 2011 <http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html#ixzz2hOpjMQ1L> and AAP, 'Vodafone website exposes customer details', *ZDNet* (online), 9 January 2011 <http://www.zdnet.com.au/vodafone-website-exposes-customer-details-339308437.htm>.

826 *Vodafone OMI Report*, above n 333.

827 Peter Martin, and Lucy Battersby, 'Vodafone may be liable on privacy breach', *The Sydney Morning Herald* (online), 10 January 2011

commenced an own motion investigation in early January 2011.[828] A Request for Information Letter, similar to the Telstra Mail Out RFI Letter, was sent on 10 January 2011.[829] At the same time, the Commissioner issued a Media Release confirming it was investigating the incident.[830] Vodafone responded to the Commissioner's RFI by letters dated 14 and 19 January, 2011.[831] The second letter presumably attached a detailed account of the incident, because it comprises 98 pages. All of the contents of each of these letters and a draft letter from Vodafone to the Privacy Commissioner dated 14 January 2011 were redacted.

Some information was received by the OAIC from a third party on 21 January 2011, which is described in the list prepared in response to the FOI request as 'internal email thread re: fraud and dishonesty complaint.'[832] Although the internal email thread suggested this information was considered as part of the information relevant to the investigation, it is not clear what that information comprised or the extent to which it was considered by the Commissioner when coming to the conclusion referred to in the final OMI report.

This investigation was completed speedily, in around five weeks. A media release announcing the conclusion of the investigation, the terms of which were also agreed with Vodafone,[833] was issued on 16 February 2011, the same date as the

---

<http://www.smh.com.au/technology/security/vodafone-may-be-liable-on-privacy-breach-20110109-19jup.html>. 94% of the 7744 votes were 'yes'.

828 The OMI report states that the Commissioner opened the investigation "in response to media reports that the personal information of Vodafone Hutchison Australia (Vodafone) customers had been compromised." *Vodafone OMI Report*, above n 333, 1.

829 Letter from Timothy Pilgrim OAIC to Vodafone, 10 January 2011 ('*Vodafone RFI Letter*'). A copy of that letter is included in Appendix C.

830 Office of the Australian Information Commissioner, 'Australian Privacy Commissioner to Investigate Vodafone Allegations' (Media Release, 10 January 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-to-investigate-vodafone-allegations>.

831 Letter from CEO, Vodafone to Timothy Pilgrim, 14 January 2011; Letter from CEO, Vodafone to Timothy Pilgrim, 19 January 2011.

832 Emails, 20 January 2001 to 21 January 2011; attached to letter from Caren Whip, OAIC to Jodie Siganto, 30 August 2013, scheduled item: Document Schedule B_Vodafone 10.

833 Email from Linda King, OAIC to Vodafone, 15 February 2011; attaching draft undertakings and media release.

publication of the OMI report.[834] Although commenced after the Telstra Mail Out investigation, the Vodafone report was completed and published before the *Telstra Mail Out OMI Report* was released.

In the OMI report, Vodafone is found not to have breached NPP 2 but to have failed to take reasonable steps to protect information for the purposes of NPP 4.1. The decision in regard to NPP 2 turned on whether personal information was 'generally accessible.' The OAIC seems to have considered only the possible disclosure that had been reported in the press. Based on that report, one user (presumably the journalist involved) was given access to his own personal information in the Vodafone data base. In those circumstances it was open to the OAIC to find that their Vodafone customer information was not publicly available on the internet or on the Vodafone website, nor was any Vodafone customer information disclosed to any third parties.

The findings in regard to NPP 4 are considered further in the next chapters.

### 8.1.3 Sony PlayStation Network/Qriocity

The Privacy Commissioner's own motion investigation into whether there had been any breach of the *Privacy Act* by Sony PlayStation and Qriocity networks commenced in 27 April 2011.[835] It was prompted by extensive media reporting of an attack on the Sony PlayStation Network (PSN) resulting in the compromise of information in relation to approximately 77 million PSN customers around the world.[836] Problems with the PlayStation Network came to light when Sony closed

---

834 Office of the Australian Information Commissioner, 'Privacy Commissioner Releases Investigation Findings' (Media Release, 16 February 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-releases-vodafone-findings>.

835 The *Sony OMI Report*, above n 335, refers to the investigation being commenced 'following media reports'. The investigation also included copies of two media reports: 'Playstation hacking scandal: police chief says contact your bank now', *Sydney Morning Herald*, 27 April 201; and 'PlayStation privacy breach: 77 million customer accounts exposed', *Sydney Morning Herald*, 27 April 2011.

836 See, eg, Chris Griffith and Karen Dearne, 'Breach sparks security alert: call for laws to protect against Playstation-style attacks', *The Australian IT* (online), 3 May 2011 <http://www.theaustralian.com.au/australian-it/breach-sparks-security-alert-call-for-laws-to-protect-against-playstation-style-attacks/story-e6frgakx-1226048705602?referrer=email&source=AIT_email_nl&emcmp=Ping&emchn=Newsletter&em

down access to the PSN on 20 April 2011. Users attempting to sign in were advised that the PSN was 'undergoing maintenance.' It was not until 25 April that Sony admitted that there had been an 'external intrusion' which had affected the PSN[837] and that it had brought in external experts to assist in the forensic analysis required to help understand the cause and scope of the breach.[838] At the time of the incident and subsequently while the Commissioner's investigation was proceeding, Sony did not release any detail describing how the attack had been carried out. However, it was widely considered that the attack was the work of an internet vigilante group that had vowed retribution against Sony for taking legal action against hackers who had cracked PS3 defences to change console operating software, and who had announced earlier that month its 'Operation Payback' campaign aimed at Sony.[839]

On opening the investigation, the Commissioner issued a statement[840] and sent an RFI Letter to Sony Australia.[841] Sony Australia responded on 11 May 2011, which

---

list=Member>; Liana Baker, 'Sony PlayStation suffers massive data breach', *Reuters* (online) 26 April 2011 <http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>; 'Sony bows head over PlayStation security breach' *The Sydney Morning Herald* (online), 2 May 2011 <http://www.smh.com.au/technology/security/sony-bows-head-over-playstation-security-breach-20110502-1e3m5.html#ixzz2g95KsFNE>; Cliff Edwards, Karen Gullo, and Michael Riley, 'Sony Faces Lawsuit, Regulators' Scrutiny Over PlayStation Breach' *Bloomberg* (online) 28 April 2011 <http://www.bloomberg.com/news/2011-04-28/sony-faces-lawsuit-regulators-scrutiny-over-playstation-user-data-breach.html>.

837 Ibid. Jared Carstensen, 'Sony PlayStation Hack: 70 Million Users' Details Stolen', *InfoSec Island* (online) 27 April 2011<http://www.infosecisland.com/blogview/13337-Sony-PlayStation-Hack-70-Million-User-Details-Stolen.html>. See also the U.S. House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade, 'Hearing on "Sony and Epsilon: Lessons for Data Security Legislation,"' (2 June 2011) <http://democrats.energycommerce.house.gov/index.php?q=hearing/hearing-on-sony-and-epsilon-lessons-for-data-security-legislation-subcommittee-on-commerce-m>; 'PlayStation privacy breach: 77 million customer accounts exposed', *The Sydney Morning Herald* (online), 27 April 2011.

838 Steve Musil, 'Senator slams Sony's response to security breach', *Cnet* (online), 3 May 2011 <http://www.cnet.com/news/senator-slams-sonys-response-to-security-breach/>; and Tim Kelly, 'Analysis: Sony bungles data breach response', *IT News* (online) 28 April 2011 <http://www.itnews.com.au/News/255788,analysis-sony-bungles-data-breach-response.aspx>.

839 See, eg, Dean Takahashi, 'Hacktivist group Anonymous launches "payback" cyber-attack on Sony', *VB News* (online) 3 April 2011 <http://venturebeat.com/2011/04/03/hacktivist-group-anonymous-launches-payback-cyber-attack-on-sony/>.

840 Office of the Australian Information Commissioner, 'Investigation into Sony Breach: Statement of the Australian Privacy Commissioner, Timothy Pilgrim' (Statement, 4 May 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/sony-playstation-network/investigation-into-sony-data-breach-4-may-2011>.

response was fully redacted.[842] A file note recorded details of an internal OAIC meeting held on 12 May 2011 following receipt of the Sony Australia response, at which it was '[a]greed appears no breach of NPP4. Will do some research re whether if something is stolen it amounts to a disclosure under NPP2 and will discuss again on Monday 16 May.'[843] There was little further activity until a draft Closing Letter and OMI report were sent to Sony for their review on 29 June 2011.[844] Again, the contents of these documents have been redacted in full.

Sony Australia responded on 8 July 2011.[845] Although this letter has also been redacted it would seem that Sony Australia raised jurisdictional issues regarding the application of the *Privacy Act*, suggesting in particular that the local Australian entity had not collected or held any personal information.[846] Further discussion in regard to jurisdiction resulted in an updated draft Close Letter and OMI report being sent to Sony for its review on 15 September.[847] These documents were finalised and issued by the end of September,[848] together with a media release advising of the conclusion of the investigation.[849]

---

841 Letter from Timothy Pilgrim to Sony's Managing Director, 27 April 2011 ('*Sony RFI Letter*').

842 Email from Sony to AM (OAIC), 11 May 2011.

843 See Office of the Australian Information Commissioner, 'Case Management Summary: Sony Computers Entertainment Australia Pty Ltd' (18 June 2013) ('*Sony Case Management Summary*'), attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Document Schedule B_Sony 1, this document contains a reference to this meeting on May 12, 2011. No record of the meeting was produced by the OAIC pursuant to the FOI Request.

844 Email from OAIC to Sony, 29 June 2011; enclosing draft OMI report: Header: 'FINAL Sony 1 Own Motion Investigation Report June 2011 ('*Sony Close Letter'*).

845 Email from Sony to LK, OAIC, 8 July 2011; with attachments – OAIC draft report and draft close letter from Privacy Commissioner with SCEE suggested amendments.

846 According to the published *Sony OMI Report*, above n 335, Sony Computer Entertainment Europe ('*SCEE'*) is the data controller for the PSN/Qriocity personal data – and is the entity that had collected the personal information of Australians.

847 Email from LK, OAIC to SCEE, 14 September 2011; re Final Investigation Report – apology for delay and comments – with attachments – Sony Final Investigation Report (draft format).

848 Letter from Timothy Pilgrim (signed) to Managing Director, Sony, 29 September 2011.

849 Office of the Australian Information Commissioner, 'Australian Privacy Commissioner Concludes Sony Investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation>.

The *Sony OMI Report* found that there was no evidence of any disclosure because there was no positive act of disclosure by Sony; 'rather the information was accessed as a result of a sophisticated security cyber-attack against the Network Platform.' It also found that Sony had taken reasonable steps to secure the personal information for the purposes of NPP 4. An analysis of the findings regarding compliance with NPP 4 is included in the next two chapters.

Much is made in the report of the delay in notifying of the breach and the method used. It was noted that the OAIC believed that 'affected individuals could have been notified earlier' and that the delay in notification may have increased the risk of a misuse of the individuals' personal information.[850] These comments were relevant in view of the then-current discussions around the introduction of mandatory data breach notification requirements (which introduction was supported by the OAIC).[851] However, the report does not attempt to place data breach notification as part of the Commissioner's consideration of whether Sony had taken reasonable steps for the purposes of NPP 4.

The report also referred to the jurisdiction issues raised by the incident, because Sony Australia (the entity covered by the *Privacy Act*) did not hold the personal information. The report states that in recognition of the challenges posed by global companies operating out of different jurisdictions, the Privacy Commissioner would provide a copy of the report to privacy regulators in the APEC member economies, for their consideration. It is not clear whether this happened or whether there were any consequences.

### 8.1.4 Telstra Bundles

On December 9, 2011, a Whirlpool forum user discovered he could access a Telstra tool (called the 'visibility tool') that was meant to be available only to Telstra

---

850 *Sony OMI Report*, above n 335.

851 See e.g. Darren Pauli, "Data breach laws to follow privacy reforms' *ITNews* (online), 4 October 2011 <http://www.itnews.com.au/News/275598,data-breach-laws-to-follow-privacy-reforms.aspx> which refers to interest by the then Minister for Privacy in passing mandatory data notification laws.

employees to enable them to search internal customer records via a Google search.[852] A screen shot from the tool is shown in *Figure 6*. The tool enabled access to information about a Telstra customer's Bundle orders, including their plan, billing account numbers, first and last names and notes about their account including, in many cases, their usernames and passwords. Users on the Whirlpool forums confirmed that their own details and accurate information such as addresses, passwords and mobile numbers had been stored in account notes.[853]

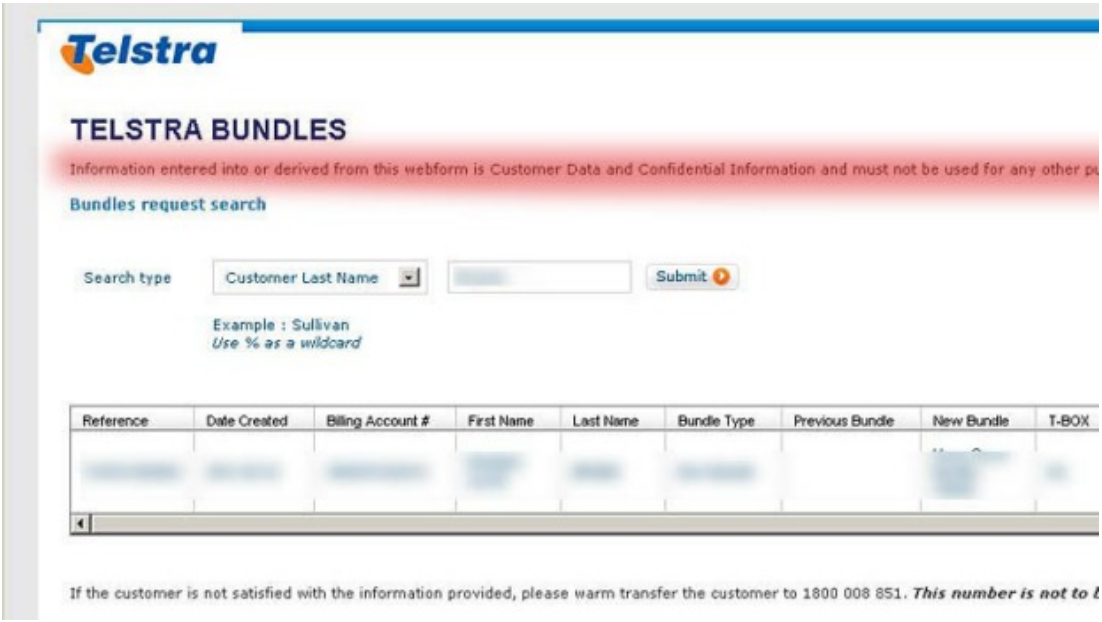



*Figure 6: The Tool accessible via the exposed url*[854]

The front page of the visibility tool carried a warning (apparent from the copy included in *Figure 6* above) that the information was 'Customer Data and Confidential Information.' According to the report from the Commissioner's investigation at the time of the incident, the visibility tool could only be accessed by an individual who had the specific url for the visibility tool. However, the url could be discovered in a number of ways:

---

852 See, eg, Asher Moses and Ben Grubb, 'Telstra Customer database exposed', *The Sydney Morning Herald* (online), 9 December 2011 <http://www.smh.com.au/it-pro/security-it/telstra-customer-database-exposed-20111209-1on60.html>,

853 WireFire, 'Our Best Ever Cable Broadband Deal' on *Whirlpool Forum* (9 December 2011) <http://forums.whirlpool.net.au/forum-replies.cfm?t=1801978&p=27#r533>.

854 Moses and Grubb, above n 854.

- By conducting a specific search on Google using a number that should not have been made publicly available, or
- By entering the search term 'help Telstra bundles', or
- By entering the URL that was available for a short period from the posting to the Whirlpool forum in their browser window.[855]

Access to the visibility tool exposed the details of 734,000 Telstra Bundles customers.[856] Shortly after the posting to the Whirlpool forum, attempts to access the tool were blocked by Telstra, which also issued an apology and a confirmation that 'Telstra takes its customers [sic] privacy seriously.'[857]

On 12 December 2011, the Commissioner opened an own motion investigation reported to be 'in response to allegations that [Telstra] had breached customer privacy by making its web-based customer management tool publicly available on its website.'[858] Telstra had notified the OAIC of the breach on 9 December 2011. In the notification, Telstra confirmed that, as soon as it had discovered the breach, it had disabled access and reset the passwords of those affected, and that it was undertaking a full investigation using an external provider and that a copy of the report and full details of the incident would be provided.[859] Telstra provided the OAIC with a further briefing about the event via teleconference on 12 December 2011, following which an RFI Letter was sent by the OAIC.[860] The OAIC also issued a statement confirming that it was undertaking an investigation.[861]

---

855 *Telstra Bundles OMI Report,* above n 336.

856 Ibid.

857 According to media reports, at about 4.45pm AEDST, about an hour after Telstra was notified of the breach by this website, customer details were still accessible. At about 5pm AEDST the site presented internet users with 'Access Denied'. See Moses and Grubb, above n 854.

858 *Telstra Bundles OMI Report*, above n 336.

859 Email from Telstra to Timothy Pilgrim, OAIC, 9 December 2011.

860 Letter from Mark Hummerston, Assistant Commissioner Compliance, OAIC to Telstra, 12 December 2011 ('*Telstra Bundles RFI Letter*').

861 Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy Commissioner opens investigation into Telstra customer accounts data breach' (Statement, 12 December, 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/telstra-data-breach/>.

Perhaps as a result of the earlier briefing, the questions included in the Telstra Bundles RFI Letter were different to those posed in the previous investigations.[862] The letter asked for a response by 13 January 2012. Telstra indicated that it would require more time,[863] and the OAIC agreed to an extension to the end of January.[864] On 3 February 2012 Telstra emailed two reports to the OAIC: 'Telstra response to Own Motion investigation C15983:tj' and 'Telstra Bundles Visibility Tool Incident Report.'[865] Both of these reports were fully redacted. A file note from an internal OAIC meeting held following receipt of these reports indicates they were not considered adequate. It was '[a]greed to ask further questions as [it was] not a once off but [a] series of mistakes by a number of people in different roles.'[866] The further questions were to cover 'what the Compliance Questionnaire includes, what was the chain of responsibility and what processes of Privacy Impact Assessment may be/planned to be put in place.'[867] The follow-up letter sent on 8 March 2012 also requested a meeting with Telstra to 'discuss the breach and what next steps are appropriate to ensure that problems are addressed at the early stages of a project.'[868] Details of the further information sought, other than the OAIC's interest in 'examining the project's quality assurance processes' was redacted.[869]

In that letter the OAIC states that the incident may indicate that there are systemic issues within the Telstra systems with regard to data security.[870] The letter

---

862 The *Telstra Bundles RFI Letter*, above n 848, is discussed further in Chapter 9.6.

863 Email thread between Linda King, OAIC and Telstra, 14 December 2011 to 15 December 2011.

864 OAIC, File note, 15 November 2011; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 56.

865 Email from Telstra to the OAIC, 3 February 2012; this email had two attachments: Attachement 1 Telstra response to Own Motion investigation; and Attachemnt 2; Telstra Bundles Visibility Tool Incident Report. Both of the attachments to the email were redacted in full.

866 OAIC, File note, 9 February 2012; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 46.

867 Ibid.

868 Letter from Mark Hummerston, Assistant Commissioner Compliance to Telstra, 8 March 2012. A copy of this letter is included in Appendix C.

869 Ibid.

870 Ibid.

continues: 'Ultimately we would like to be able to identify all the relevant vulnerabilities that led to the incident, provide guidance on how to address them and close the matter.'[871]

Telstra responded that it would prefer to provide a written report (rather than meet) and that it would need until 30 March 2012 to do so.[872] The OAIC accepted this although noting that '[t]he Assistant Commissioner has expressed some concern at the time being taken by Telstra in responding fully to this matter.'[873] Telstra responded by an email on 26 March 2012, the contents of and attachments to which are redacted.[874] A follow-up teleconference between representatives of Telstra and the OAIC occurred on 29 March 2012, at which it was agreed that Telstra would send information about their 'new plan for reasonable steps before Easter.' The file note from that call records that it was agreed that there was a breach of NPP 2.1 and NPP 4. The file note further provides: 'Aim is to be able to say that there was a breach but also that Telstra is adequately dealing with it and bringing reasonable steps into place.'[875] Further information on the remediation steps was provided by email on 5 April 2012,[876] on receipt of which the OAIC began drafting the Close Letter and the OMI report. There was a further relatively minor query from the OAIC on 13 April 2012.[877] A Close Letter was sent via email on April 30 2012,[878] to which Telstra responded with comments and corrections,[879] and a draft of the OMI

---

871 Ibid.

872 OAIC, File note, 15 March 2012; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 36. Email thread between OAIC and Telstra, 15 March 2012.

873 Email thread between OAIC and Telstra,15 March 2012.

874 Email from Telstra to OAIC, 26 March 2012.

875 OAIC, File Note, 29 March 2012; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 30.

876 Email thread from Telstra to TJ, 5 April 2012.

877 Email thread from OAIC to Telstra, 13 April 2012.

878 Email thread from TJ, OAIC to Telstra, 30 April 2012 ('*Telstra Bundles Close Letter'*).

879 Email thread from Telstra to TJ, OAIC, 3 May 2012.

report was sent on 8 June 2012.[880] The final OMI report was then issued in July 2012, together with a media release.[881]

The Privacy Commissioner asked for a report on the progress of the remediation project six months from the date of the Close Letter and another no later than 12 months from the date of the Close Letter.[882] In November, 2012 the six-month report was provided by Telstra to the OAIC.[883] There was no indication from the documents provided that the 12-month report due in June 2013 had been requested or provided.

The OMI report, like those issued in regard to the other investigations, details Telstra's response to the incident, including that it had immediately set up an Incident Response Team, disabled online access to the tool (including cached copies), contacted relevant regulators (the OAIC, the ACMA and the Telecommunications Industry Ombudsman) and took a series of other actions, including resetting passwords and notifying affected customers.[884] The report notes how the incident occurred and that Telstra was informed in November 2011 (at least a month before the incident) that the visibility tool was accessible externally and was not protected by the Telstra firewall. No action was taken at that time to escalate this alert to the appropriate internal Telstra business areas.

Telstra identified two key causes of the incident:

- An incorrectly completed compliance questionnaire[885] - an early failure by a project manager to correctly complete a compulsory internal questionnaire

---

880 Letter from Mark Hummerston, Assistant Commissioner Compliance to Telstra, 8 June 2012.

881 Office of the Australian Privacy Commissioner,'Telstra Breaches *Privacy Act*' (Media Release 29 June 2012) < http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-act>.

882 OAIC, File note, 9 May 2012; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 8.

883 Email from AF, OAIC to Telstra, 1 November 2012.

884 *Telstra Bundles OMI Report,* above n 336.

885 This questionnaire seems likely to be the questionnaire that was subject to further review by the OAIC.

required to determine the necessary security profile of a new project relating to the recording of Telstra customer bundle orders; and

- Failure to follow proper systems, processes and oversight — subsequent failures by the project team tasked with developing and implementing the visibility tool to raise relevant privacy and security risks outside the project team.

According to the report, Telstra committed to extensive remedial actions, including an audit of all of its applications, revision of its Privacy Compliance Program, implementation of a new internal training program, enhancement of existing processes and establishment of a system where the Chief Privacy Officer is involved in the management of incidents concerning privacy.[886]

The Commissioner's investigation focused on whether the incident was an 'unauthorised disclosure' of personal information (and a breach of NPP 2) in addition to a failure to take reasonable steps to protect personal information (and a breach of NPP 4). It concluded that specific errors by Telstra staff led to the visibility tool being publicly accessible and that that external access to customers' personal information was an unauthorised disclosure and therefore a breach of NPP 2.1. The Commissioner then considered whether there had been a breach of NPP 4, finding that although Telstra had existing policies and procedures in place that, if followed, would have prevented the errors that led to this incident, there was evidence of behaviours not consistent with those policies and procedures. On this basis, the Commissioner found that Telstra did not have reasonable steps in place with regard to data security in the visibility tool in compliance with NPP 4.1.[887]

The Commissioner noted that Telstra took appropriate steps to investigate the incident, notify affected customers and contain the breach; and, at the time of the Commissioner's investigation, was implementing a comprehensive review of its

---

886 *Telstra Bundles OMI Report*, above n 336.

887 *Telstra Bundles OMI Report*, above n 336.

security systems. These steps aimed to mitigate the effects of the breach and ensure that no further unauthorised access occurred.[888]

There is no reference in the report to Telstra having any systemic issues in regard to privacy or the protection of personal information pursuant to NPP 4.

### 8.1.5 Dell Australia / Epsilon

Epsilon is a 'leading provider of permission based email marketing services' having over 2500 customers, which include some of the 'world's largest and best-known consumer and financial brands.'[889] It reportedly sends over 40 billion emails a year.[890]

At some time prior to 30 March 2011, an attacker used an Epsilon employee's credentials, captured via malware downloaded by the employee via the internet, to log on to Epsilon's email marketing platform and gain access to the names and email addresses of customers of over 60 Epsilon client companies including Dell Australia.[891] The employee reported unusual download activity in late March, which led to Epsilon becoming aware of the unauthorised access. In addition to action to halt the compromise and forensically determine its source, Epsilon gave notice of the breach, telling its clients on April 1 that a 'subset' of client data had been exposed by an unauthorised entry to its email system. It also set up an incident response centre, added information to its website, and informed U.S. law enforcement and undertook its own investigation. [892] After the breach, there were

---

888 Ibid.

889 Prepared Statement of Jeanette Fitzgerald, General Counsel, Epsilon Data Management before the House Committee on Energy & Commerce, Subcommittee on Commerce, Manufacturing and Trade, U.S. House of Representatives, 2 June 2011 ('*Fitzgerald Statement*')

890 'Security breach widens at US retailers', *The Australian* (online), 4 April 2011; and Asher Moses, 'Dell Australia customer details stolen in major data breach', *The Sydney Morning Herald* (online), 7 April 2011 <http://www.smh.com.au/technology/security/dell-australia-customer-details-stolen-in-major-global-data-breach-20110407-1d4yd.html#ixzz2gWxiBHkk>.

891 Based on the facts referred to in the *Dell/Epsilon OMI Report*, above n 337. See also *Fitzgerald Statement*, above n 889, 13.

892 See *Dell/Epsilon OMI Report*, above n 337; *Fitzgerald Statement*, above n 889, 13 – 14.

media reports that the attack was of the same type that email houses had been warned about four months previously.[893]

The records obtained for the Dell/Epsilon investigation were the most incomplete due to the omission of the separate file holding records of the Epsilon investigation from the original decision.[894] A number of important records from the Epsilon investigation file had not been provided as at 30 March 2014.[895] The following details of the investigation are based on the information available as at 30 March 30 2014.

Dell Australia notified its customers and the Commissioner of the breach on 6 April 6 2011.[896] The incident affecting Dell was reported in the Australian press on the same date.[897] Shortly thereafter it was reported that the Privacy Commissioner would be investigating the breach.[898]

An internal OAIC email sent on 7 April 2011 referred to asking Epsilon for a copy of their investigation report (once completed) and 'a list of any Australian companies who use Epsilon's services and had data accessed through the breach.'[899]

Separate RFI Letters were sent to DA and Epsilon.[900] Both organisations responded in mid-May,[901] presumably both advising that they were still investigating

---

893 Brett Winterford, 'Epsilon breach used four-month-old attack', *ITNews* (online) 7 April 2011 <http://www.itnews.com.au/News/253712,epsilon-breach-used-four-month-old-attack.aspx>.

894 See the discussion of the freedom of information process in Chapter 4.3.2.

895 These include the request for information letter sent by the OAIC to Epsilon. Some of these records were disclosed by the OAIC after 30 March 2014 however they have not been considered in this research.

896 Email from Dell, 6 April 2011; Letter from Dell to Timothy Pilgrim, 6 April 2011.

897 Karen Dearne, 'Dell Australia Impacted by Epsilon email breach', *The Australian IT* (online), 6 April 2011; and Campbell Simpson, 'Dell Customer email addresses accessed in Epsilon Breach' *CSO* (online), 6 April 2011.

898 See, eg, Karen Dearne, 'Privacy czar to investigate Epsilon email breach', *The Australian* (online), 7 April 2011 < http://www.theaustralian.com.au/technology/privacy-czar-to-investigate-epsilon-email-breach/story-e6frgakx-1226035569602#sthash.w4iypq2o.dpuf> Asher Moses, 'Dell Australia customer details stolen in major data breach', *The Sydney Morning Herald* (online), 7 April 2011<http://www.smh.com.au/technology/security/dell-australia-customer-details-stolen-in-major-global-data-breach-20110407-1d4yd.html#ixzz2gWxiBHkk>.

899 Email chain, OAIC, 7 April 2011.

the incident because, in July, the OAIC sought updates from both DA and Epsilon on their respective incident reports.[902]

DA advised on 19 July that it had completed a 'high level off-site' security assessment of some part of Epsilon's infrastructure but it had not been able 'to complete an onsite audit of the corrective and preventative actions taken by Epsilon … because the incident is still under investigation by law enforcement authorities in the United States.'[903] Epsilon provided a copy of the investigative report prepared for it in mid-November (after securing appropriate confidentiality undertakings from the OAIC).[904] The Cases against both DA and Epsilon were closed in January 2012[905] and drafts of the OMI report and Closing letters were sent in July 2012.[906]

No media release was issued at the conclusion of the case.

The OMI report published in July 2012 only considers whether there was a breach of NPP4.1. There was no consideration of whether there had been a breach of NPP2 or any other principle – including NPP9 (which may have applied in the context of any cross-border transfer of data). This is notwithstanding that the Complaints Assessment Sheet for the Dell data breach notification investigation file refers to both NPP 2 and NPP 4 in the 'Complaints Code' section of the form.[907]

The Dell/Epsilon OMI is similar to the Sony OMI in a number of ways:

---

900 Letter from Mark Hummerston, OAIC to Dell, 19 April 2011 ('*Dell RFI Letter*'). Email from MS, OAIC to Epsilon. Copies of these documents are included in Appendix C.

901 Email thread from MH, OAIC to MS, 11 May 2011. A copy is included in Appendix C. Email from Epsilon to MS, OAIC, 16 May 2011 (this document was referred to in the list of documents but no copy was made available prior to 20 March 2014).

902 Email thread between OAIC and Dell, 5 July 2011; Email from OAIC to Epsilon, 1 July 2011.

903 Email from Dell to MS, OAIC, 19 July 2011. A copy is included in Appendix C.

904 Email thread from Epsilon to AM, OAIC, 15 November 2011.

905 Letter from Mark Hummerston, OAIC to Dell, 11 January 2012 ('*Dell Close Letter*'). Email thread from AM, OAIC to Epsilon, 11 January 2012.

906 Letter from Mark Hummerston, OAIC to Dell, July 2012 (unsigned). Letter from Mark Hummerston, OAIC to Epsilon, 2 July 2012 (signed).

907 Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet – DBN, 6 April 2011 ('*Dell DBN CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Dell 26.

- In both cases, the incident was referred to as 'a sophisticated and malicious attack which required expert knowledge to execute;'
- As in the Sony investigation, Epsilon's range of security measures in place were found to be sufficient for the purposes of NPP 4.1, although reference was also made to a number of enhancements implemented following the breach; and
- Jurisdictional issues were raised, in this case in regard to the application of the *Privacy Act* to Epsilon (being a US incorporated organisation, and arguably not carrying on business in Australia). Again, because the Commissioner was satisfied that Epsilon had met its obligations under the NPPs the Commissioner was not required to reach a formal view on this matter.

The Commissioner decided to cease the investigation into the incident, noting with approval how quickly Epsilon had acted to contain risks to the personal information and to 'take appropriate steps to investigate the incident, improve its security systems further and work with law enforcement agencies regarding this matter.'[908]

### 8.1.6 Medvet Science Pty Ltd

The report on the own motion investigation into Medvet was published in July 2012, just over a year from the date that the events were first made public in an 'exclusive' article published in The Australian newspaper.[909]

Medvet is a private company owned by the South Australian government which offers a 'comprehensive range of cost-effective health and safety services' including drug and alcohol testing and DNA paternity testing. [910] Drug and DNA self-testing kits could be ordered via a Medvet webpage and delivered directly to the

---

908 *Dell/Epsilon OMI Report*, above n 337, 2.

909 Hedley Thomas, 'DNA test names exposed online', *The Australian* (online), 16 July 2011 < http://www.theaustralian.com.au/news/health-science/dna-test-names-exposed-online/story-e6frg8y6-1226095576596 >.

910 From Medvet Science Pty Ltd, *About Us* <http://www.medvet.com.au/about-us>.

nominated shipping address. Medvet's website was hosted by CP Moore, who reportedly used an ecommerce application (called Webstore) developed by another party, Iciniti Corporation, to support online purchasing of the test kits.[911]

The press seem to have been alerted to the incident by an anonymous 'industry figure' who, according to the reports, had advised South Australia Health (the owners of Medvet) of the issue in April (some three months earlier).[912] The first media contact was on Friday 13 July 2012, with the article publishing details of the online availability of personal information appearing on Monday 16 July 16 2011 (see *Figure 7*). From 16 July 16 2011 the event received significant attention from the media.[913]

The headline of the initial press report suggested that the names of people who had ordered DNA tests were exposed online; however, all subsequent reports referred only to delivery details being available.[914] Medvet advised the Privacy Commissioner that the information was limited to the 'ship to address' from each order, details of the service/product requested and the price paid for that service/product. No customer names, client bank account details or details of any test results were available online.[915]

---

911 C.P. Moore Business Solutions, *About Us* <http://www.cpmoore.com/About_Us.aspx>.

912 Thomas, above n 911, which states that the Medvet CEO 'initially said he had no knowledge of a recent previous security issue at Medvet's web store. When The Weekend Australian told him it was aware the matter had been brought to his attention earlier this year, he acknowledged it and said he instituted action at the time to fix the problem.'

913 See, eg, Sarah Martin 'Investigation into South Australia's Medvet lab after serious privacy breach', *The Advertiser* (online), 18 July 2011 <http://www.news.com.au/national-old/south-australias-medvet-blood-lab-publishes-details-of-paternity-and-drug-test-applicants/story-e6frfkx9-1226096476780>. 'Online medical privacy breach to be probed', *ABC News* (online) 18 July 2011 <http://www.abc.net.au/news/2011-07-18/medvet-privacy-breach-online/2798650>.

914 Thomas, above n 911.

915 *Medvet OMI report*, above n 338.

| Bill To | | Ship To | |
|---|---|---|---|
| | , | | MATRAVILLE NSW<br>AU 2036 |

| Qty | Unit | Product | Description | Shipped | Back Ordered | Invoice Date | Unit Price | Price |
|---|---|---|---|---|---|---|---|---|
| 1 | Each | SC1 PAR | SELF COLLECT PATERNITY TEST | 1 | 0 | Jan 10/2011 | $320.00 | $320.0 |
| 0 | | | Shipping charge | 0 | 0 | Jan 10/2011 | $0.00 | $0.0 |

| | |
|---|---|
| Subtotal | $0.00 |
| GST | $0.00 |
| Miscellaneous | $0.00 |
| Total | $0.00 |

*Figure 7: An example of the details of one of the orders for a Paternity Test that was available online.*[916]

An OMI investigation was opened on 18 July 2011 following a press report on 15 July 2011 in which the Commissioner stated that 'it would launch a formal 'own motion' investigation.'[917] On opening its investigation, there was an initial discussion regarding whether the *Privacy Act* applied to Medvet, as a corporation wholly owned by the South Australian government.[918] Finding that it did apply, the Commissioner sent an RFI Letter on July 20, 2011, which was in similar terms to that issued to Sony.[919] Medvet responded by letter on 11 August 201, the contents of which have been redacted in full.[920] In early September, the Commissioner's office

---

916 Asher Moses, 'Paternity and drug test details leak online in privacy breach', *The Sydney Morning Herald* (online) 18 July 2011 <http://www.smh.com.au/technology/security/paternity-and-drug-test-details-leak-online-in-privacy-breach-20110718-1hkyn.html#ixzz2EiZDNyiV>.

917 Thomas, above n 911.

918 Letter from Mark Hummerston to Medvet, 18 July 2011 (not provided as part of the disclosed records). There is also reference to a phone call with the respondent and an email response to the queries but these records was not provided by 30 March 2014, see Office of the Australian Information Commissioner, 'Case Management Summary: Medvet Laboratories' (20 June 2013) ('*Medvet Case Management Summary*'), attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Document Schedule B_Medvet 1.

919 Letter from Timothy Pilgrim to Medvet, 20 July 2011 ('*Medvet RFI Letter*'). A copy of this document is included in Appendix C.

920 Email from Medvet to AM, OAIC, 11 August 2011.

queried the availability of a report into the incident being prepared by Deloitte.[921] A copy of a Medvet Press Release about the Deloitte report and a copy of the report were forwarded to the Commissioner's office.[922] On 11 October, the case officer noted that '… we received a response from Medvet on 21 September and I have assessed the response and it appears that R has taken reasonable steps and we are in a position to finalise.'[923] That same file note also referred to discussing the matter further internally at the OAIC before drafting a close letter because 'TP may want to do a report as it was in the media.'

In November, the Commissioner's office checked with Medvet on the implementation of the changes that were presumably recommended in the Deloitte report provided in September.[924] Medvet advised that it had retained a third party to prepare a report on the implementation.[925] An internal email confirmed that the OAIC would pursue receipt of this second report even though '[i]f the report is highly technical it may not assist us anyway.'[926]

It seems that the implementation report was provided to the OAIC around 5 December 2011, although again no correspondence relevant to the provision of this report was included in the FOI documents produced.[927]

---

921 Email from AM, OAIC to Medvet, 5 September 2011.

922 Email thread from Medvet to AM, OAIC, 21 September 2011. The Deloitte Report is not included as an attachment to this email threat (and was not disclosed). The Report is not referred to in any other correspondence.

923 OAIC, File note, 11 October 2011; referred to in *Medvet Case Management Summary*, above n 920.

924 OAIC, File note, 4 November 2011; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Medvet 11; 'looking to see if changes have been implemented and get a copy of the forensic report. Will call on Monday.' OAIC, File note, 8 November 2011; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Medvet 12.

925 OAIC, File note, 9 November 2011; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Medvet 9.

926 OAIC, File note, 19 November 2011; attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Medvet 5.

927 The records refer to a Letter from Medvet MD to OAIC, 28 November 2011, which may have included the implementation report, but this has been redacted.

A closing letter signed by Mark Hummerston, the Assistant Commissioner, was sent to Medvet on 19 December, 2011.[928] The content of that letter has largely been redacted and it is not clear whether or not Medvet was found to be in breach of either NPP 2 or NPP 4, although a later letter from the Commissioner indicated that the finding was that only NPP 4 had been breached.[929] In the December 2011 letter, Mark Hummerston noted that Medvet 'acted swiftly to identify the security risks to the personal information it holds and has taken appropriate steps to improve its security systems and develop policies and procedures that reduce identified risks.' In light of that and the security measures being implemented, he advised that the investigation would cease and the file on this matter 'is now closed.'

According to the file, a draft OMI report was prepared and sent to Medvet for comment in May 2012 (nearly 5 months after being advised that the file was closed).[930] No record of that correspondence had been disclosed as at March 30, 2014. Although there is no reference to any further interaction between the OAIC and Medvet on the file, in July 2012 the Commissioner advised Medvet that, 'as it was aware,' the Commissioner had reviewed the file and as part of that review had determined that there was a breach of NPP 2, as well as NPP 4.[931] The reasons for that decision are redacted in full. Attached to this letter is a draft OMI report presumably describing a different outcome to the draft OMI report that had been sent in May 2012. The finding of breach of both NPP 4 and NPP 2 are consistent with the OMI report that was published on the OAIC website on 26 July 2012 (and different to the findings that seem to have been communicated in December 2011).

In terms of NPP4, the OMI report refers extensively to the findings in the Deloitte report, stating that 'it was clear from the Deloitte's forensics report that multiple security flaws existed in the software provided by Iciniti and hosted by CP

---

928 Letter from Mark Hummerston, Assistant Commissioner, OAIC to CEO Medvet, 19 December 2011 ('*Medvet Close Letter 1*').

929 Letter from Timothy Pilgrim, Privacy Commissioner to CEO Medvet, 10 July 2012 ('*Medvet Close Letter 2*'). A copy of this letter is included in Appendix C.

930 Email from KO, OAIC to Medvet, with attachments – covering letter and Medvet OMI Investigation Report (Draft) (this document was not disclosed as at 30 March 2014).

931 *Medvet Close Letter 2*, above n 929.

Moore,'[932] and therefore Medvet was putting individuals' personal information, including sensitive health information, at risk of being compromised. Based on these findings, it was the Commissioner's view that Medvet did not have reasonable steps in place to protect the personal information it held at the time of the incident and therefore it did not meet its obligations under NPP 4.1.

The report goes on to note that Medvet acted swiftly to identify the security risks as soon as it became aware of the incident and that, since the incident, Medvet has taken steps to improve its security systems and develop policies and procedures that reduce identified risks.

Following publication of the OMI report, the journalist from The Australian who had first broken the story published a series of follow-up articles critical of the investigation, suggesting that it was inappropriate for the Commissioner to rely on the Deloitte report and that the 'industry figure' who had first advised of the breach had not been included in the investigation.[933] The Commissioner is reported to have responded that the Deloitte report had been 'used to confirm evidence gathered from other sources'[934] although it is not clear from the files what those sources were. The Commissioner also sent a letter to the editor responding to claims that the investigation was not rigorous or independent.[935]

## 8.2 CONCLUSION

As noted, the nature of OMI reporting changed in February 2011 when the Commissioner adopted a new mode of responding to and reporting on high-profile data breaches. From the group of 8 OMI reports published between February 2011 and April 2013, 6 have been selected for more detailed analysis. It is apparent from

---

932 Ibid.

933 Thomas, above n 909; and Hedley Thomas, 'Paternity firm slapped over privacy breach', *The Australian* (online) < http://www.theaustralian.com.au/news/investigations/paternity-firm-slapped-over-privacy-breach/story-fn6tcs23-1226435191069>.

934 Thomas, above n 933.

935 Letter from Timothy Pilgrim, Australian Privacy Commissioner, to the Editor of The Australian Newspaper, 26 July 2013 <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/medvet-investigation/privacy-commissioner-responds-to-media-claims-about-medvet-investigation>.

the description of the events giving rise to each investigation and the resulting reports, those 6 investigations were different in many ways:

- The organisations involved ranged from a local Australian organisation to a large multinational;
- The number of people whose personal information was affected ranged from 0 (in Vodafone) to possibly millions in the Sony PlayStation investigation;
- The causes of the incidents investigated ranged from 'sophisticated' cyber-attacks (in Sony and Dell/Epsilon), to a 'one-off human error' in Telstra Mail Out, to more serious failures to take reasonable steps in Vodafone, Telstra Bundles and Medvet;
- Not every case of breach of NPP 4 involved a breach of NPP 2. In Vodafone, there was a failure to take reasonable care, but no disclosure. The reverse also applied: in Telstra Mail Out there was a breach of NPP 2 but no breach of NPP 4.

However, there are also at least two commonalities between the 6 cases.

All related to incidents that were in the media at the time, or shortly after the Commissioner decided to open an investigation. Most of the OMI reports refer to the media coverage and even in those reports that do not specifically refer to media, there is evidence of media interest at the time the investigation was commenced, for example the Telstra Mail Out. The other similarity between the cases is that, in each, the Commissioner was able to close the investigation on the basis that the respondent had already, or was in the course of, taking appropriate remediation efforts to ensure that the incident did not occur again. Both of these similarities will be examined further in the next chapter.

# Chapter 9: Findings - OMI Investigation Process

The facts and the decisions made by the Commissioner in each of the 6 investigations to be analysed in detail in this Part were covered in the previous chapter. This chapter will examine in detail how each of those 6 investigations was conducted, looking at each separate phase: the initiation, evidence gathering, and communication of the decision and reporting of each case. It will analyse those investigations using the lens of the transparent, balanced and vigorous exercise by the Commissioner of its powers. The next chapter will consider the extent to which the investigations could be regarded as supporting an industry-accepted approach to information security, looking more closely at the references to accepted practice, industry standards and the OAIC's own guidance.

The investigation process mandated by the *Complaints Manual* (following the decision to commence an investigation and completion of preliminary assessment inquiries) was discussed in Chapter 7. That process includes the following steps:

- Preparing a case plan;
- Sending letters advising of the investigation (referred to in this research as 'Request for Information letters' or 'RFI Letters');
- Collecting of relevant evidence to apply the law and relevant policy to the facts of the case; and
- Finalising the case, including considering whether or not to publish a report. [936]

Consideration of the transparency, balance and vigour of the actual investigation process used in each of the 6 investigations will be based on this process as outlined in the *Complaints Manual*.

---

[936] *Complaints Manual*, above n 227.

## 9.1 DECISION TO COMMENCE AN OMI

The criteria for commencing an OMI have been discussed in Chapter 7.2. However, none of the files for any of the OMIs being reviewed contain any record of or reference to consideration of any of these stated criteria as the basis for the decision to open an OMI.

The Assistant Commissioner, after confirming that these were the relevant criteria used, referred to two 'other way[s] of opening OMIs', the first being where the office was notified of a data breach. In that case, according to the Assistant Commissioner, the office would determine if the organisation had a strategy in place to address the breach. If satisfied that appropriate steps were being taken, then the OAIC would not take any further action, although it would seek to have the organisation report on the remedial steps taken. However, 'if the report falls short in our view then at that point we'd open an Own Motion Investigation and ask some formal questions under our Own Motion Investigation power.'

Sony, Dell/Epsilon and Telstra Bundles are all cases where the organisation notified the OAIC of a breach.[937] The OAIC decided to undertake an OMI in each of these cases. This is notwithstanding that there is no suggestion in any of the files or reports relating to these investigations that the Commissioner was concerned that the organisations might not take appropriate remedial steps to recover from the breach. To the contrary, each refers to the post-breach actions taken by the respondent with approval. For example, the conclusion to the *Sony OMI Report* provides:

> The Privacy Commissioner was also satisfied with how the incident was dealt with following the breach in terms of the extra security measures that have been implemented to help protect personal information.[938]

The Telstra Mail Out investigation seems to have been instigated following a referral from the ACMA, which had received notification of the breach in its capacity as the regulator overseeing compliance with the Telecommunications Code

---

937 See Letter from Dell Australia to Timothy Pilgrim, 6 April 2011; Email from Sony to Enquiries, OAIC, 27 April 2011; Email from Telstra to OAIC, 9 December 2011.

938 *Sony OMI Report*, above n 335.

of Practice.[939] In this regard it could be treated as similar to the data breach notification cases.

According to the ACC, the other basis on which OMIs may be opened is in response to media interest. This seems to be the most likely reason for the commencement of investigations in all 6 cases under review. Each of the incidents the subject of these OMIs had received media attention.[940] Each of the investigation files contains media clippings in regard to the particular incident being investigated, demonstrating that the OAIC was aware of the media attention.[941] The Vodafone, Sony and Medvet incidents in particular had received national press attention, with the OMI reports for both these investigations identifying the media reports as the reason for opening the investigations.[942] By way of example, the first paragraph of the *Vodafone OMI Report* provides:

> The Australian Privacy Commissioner, Timothy Pilgrim opened an own motion investigation … in response to media reports that the personal information of Vodafone Hutchison Australia (Vodafone) customers had been compromised.

Unlike most previous investigations, the Commissioner elected to respond to the media reports, not only by opening an investigation, but also in a number of cases by issuing its own media release to that effect ( in regard to the Vodafone, Sony and

---

939 See Letter from Jane van Beelen to Olya Booyar, The Australian Communications and Media Authority, 27 October 2010.

940 Natalie O'Brien, 'Mobile security outrage: private details accessible on net', *The Sydney Morning Herald* (online), 9 January 2011 <http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html#ixzz2hOpjMQ1L>; AAP, 'Vodafone website exposes customer details', *ZDNet* (online) 9 January 2011 <http://www.zdnet.com.au/vodafone-website-exposes-customer-details-339308437.htm>; Martin and Battersby, above n 827; Griffith and Dearne, above n 836; Baker, above n 836; Thomas, above n 911; Moses, above n 918; Martin, above n 915.

941 See, eg, The Dell investigation file included Excerpt from eweek.com (6 April 2011); The Australian (7 April 2011); The Sydney Morning Herald (7 April 2011); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Dell 20, 19, and 24. The Telstra Bundles investigation file included Excerpt from The Sydney Morning Herald (12 December 2011), attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Telstra 6.

942 See the references above n 940.

Telstra Bundles investigations).[943] Even in those cases where no media release was issued, the fact that the Commissioner was undertaking an investigation seemed to find its way into the public domain.[944] The Commissioner also responded to media queries about whether an investigation was being undertaken[945] and to further queries as the investigation proceeded.[946] The OAIC's continuing awareness of the on-going media interest in the investigations is demonstrated by copies of news articles held in the investigation files.[947] Specific reference to media interest was also made in correspondence between the OAIC and the respondents in the Telstra Mail Out, Vodafone and Sony cases during the course of those investigations.[948] On conclusion of the investigations, media releases were issued by the OAIC on the publication of each of the OMI reports other than for Dell/Epsilon.[949] In the Medvet

---

943 Timothy Pilgrim, 'Privacy Commissioner opens investigation into Telstra customer accounts data breach' (Statement, 12 December 2011); Privacy Commissioner 'Australian Privacy Commissioner to investigate Vodafone allegations' (Media Release, 10 January 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-to-investigate-vodafone-allegations>; Timothy Pilgrim, 'Investigation into Sony data breach' (Statement, 4 May 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/sony-playstation-network/investigation-into-sony-data-breach-4-may-2011>.

944 See, eg, Hedley Thomas, 'Privacy data still online 24 hours after alert', *The Australia* (online), 18 July 2011 <http://www.theaustralian.com.au/national-affairs/private-data-still-online-24-hours-after-alert/story-fn59niix-1226096403027#sthash.aUOZR0cJ.dpuf>, which provides that 'Privacy Commissioner Timothy Pilgrim will investigate Medvet's original internet security breach and the subsequent failure of the company to immediately remove the hundreds of customers' orders that it knew were cached by Google and online.'

945 See, eg, Karen Dearne, 'Privacy czar to investigate Epsilon email breach', *The Australian* (online) 7 April 2011 < http://www.theaustralian.com.au/technology/privacy-czar-to-investigate-epsilon-email-breach/story-e6frgakx-1226035569602#sthash.w4iypq2o.dpuf> Asher Moses, 'Telstra botched mail-out exposes 220,000 customers', *The Sydney Morning Herald* (online), 27 October 2012 <http://www.smh.com.au/technology/security/telstra-botched-mailout-exposes-220000-customers-20101027-173du.html#ixzz2hC0Ak7np>.

946 See, eg, Email thread between OAIC employees, 5 May 2011.

947 See, eg, Excerpt from smh.com.au (2 May 2011), and excerpt from smh.com.au (3 May 2011); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule B_Sony 12.

948 See, eg, Internal OAIC Email thread, 24 May 2011; which states: 'spoke to [redacted] yesterday. I confirmed we would be making a media statement accompanied by a short report upon closing the investigation.'

949 Timothy Pilgrim, 'OAIC finalises investigation into Telstra mailing list error' (Media Release, 11 October 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/oaic-finalises-investigation-into-telstra-mailing-list-error>; Timothy Pilgrim, 'Privacy Commissioner releases Vodafone Findings' (Media Release, 16 February 2011)

case, there was no media release but the Commissioner issued a statement that was published in a national paper as a letter to the editor following negative coverage of the report. [950]

The fact that the investigations and the publication of the reports on completion of those investigations may be a response to media interest (rather than, for example addressing a systemic issue) is considered later in this research in terms of the purpose of the OMI and the reasons for publishing the OMI reports.

None of the reports or investigation files refers specifically to any concern regarding systemic issues, either of a general nature affecting a particular industry or within an organisation. As referred to, the existence of systemic issues is one of the criteria for determining whether or not to undertake an OMI, and is thought to be an important use of the OMI power.[951] The only case where any reference is made to systemic issues is the Telstra Bundles investigation. The OAIC sent a letter to Telstra asking for more information about the breach (sent following the initial Telstra Bundles RFI Letter). [952] This letter states that the incident 'indicates that there may be systemic issues within the Telstra systems with regard to data security.' The letter continues, saying that the OAIC's aim is to 'identify all the relevant vulnerabilities that led to the incident, provide guidance on how to address them and to close the matter.'[953] Following this letter, there is no further reference to systemic issues in the file or in the final OMI report. However, following the release of the

---

<http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-releases-vodafone-findings>; Timothy Pilgrim, 'Australian Privacy Commissioner concludes Sony investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation>, Timothy Pilgrim, 'Telstra breaches *Privacy Act*' (Media Release, 29 June 2012) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-act>.

950 Timothy Pilgrim, 'Privacy Commissioner responds to media claims about Medvet investigation – Letter to the editor of The Australian newspaper from Australian Privacy Commissioner, Timothy Pilgrim' (Statement, 26 July 2012) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/medvet-investigation/privacy-commissioner-responds-to-media-claims-about-medvet-investigation>.

951 See Chapter 7.2.

952 Letter from Mark Hummerston, OAIC to Telstra, 8 March 2012.

953 Ibid.

*Telstra Bundles OMI Report*, the Commissioner was reported to be watching for systemic privacy weaknesses in Telstra's operational culture.[954] It is not clear what this reference to the Commissioner's interest in possible systemic issues in the media report was based on. The media release accompanying the release of the *Telstra Bundles OMI Report* contains no reference to systemic issues.[955] Nor is there any reference to systemic issues in the OMI report released in March 2014 in regard to another security failure by Telstra.[956] There is no reference to systemic issues, either as a reason for commencing the investigation or as a concern raised during the investigation, in any of the files or in the published reports for the other 5 investigations.

## 9.2 THE INVESTIGATION PROCESS

Following the decision to open an investigation, the investigation files show that the same investigation process is taken in each of the investigations. The investigation process is as follows:

- A file is set up, with a claims assessment sheet completed with the details of the investigation;[957]
- A Request for Information Letter asking that the respondent answer a series of questions about the incident is sent to the respondent, who is given a certain time period to respond;[958]
- After that response is received, it is reviewed by the OAIC. Where that response indicates that an investigation by the respondent or a third party

---

954 Andrew Colley, 'Privacy Commissioner Timothy Pilgrin will probe Telstra's culture in light of privacy breach', *The Australian* (online), 29 June 2012 <http://www.theaustralian.com.au/australian-it/telecommunications/privacy-commissioner-timothy-pilgrim-will-probe-telstras-culture-in-light-of-privacy-breach/story-fn4iyzsr-1226412092746>.

955 Office of the Australian Information Commissioner, above n 883.

956 *Telstra Bundles OMI Report*, above n 336.

957 Complaint Assessment Sheets were disclosed for all of the OMIs except Epsilon and Telstra Mail Out. These are discussed in more detail in Chapter 9.4 below.

958 Request for Information Letters were disclosed for all of the OMIs except Epsilon. There are discussed in more detail in Chapter 9.6 below.

appointed by the respondent is proceeding, the OAIC will usually follow up to ensure that it receives a copy of that report;[959]

- Once the OAIC is satisfied with the information received, and a decision has been made, a letter called a 'Close Letter' is sent to the respondent;[960] and
- Once a decision to publish a report about the investigation is made, a draft OMI report is prepared and sent to the entity for their comments and, subject to that, published on the OAIC website.[961]

This process is largely consistent with the OAIC's *Complaints Manual*[962] although there are some divergences. These are discussed in more detail in the next sections.

## 9.3 INVESTIGATION CHRONOLOGIES

The chronology for each of the above steps as they occurred in each of the 6 investigations is provided in *Table 6*.

| | **Telstra Mail Out** | **Vodafone** | **Dell/ Epsilon** | **Sony** | **Telstra Bundle** | **Medvet** |
|---|---|---|---|---|---|---|
| **Date file opened** | 27/10/10 | 10/1/11 | 7/4/11 | 27/4/11 | 9/12/11 | 18/7/11 |
| **Date RFI Letter** | 25/10/10 | 10/1/11 | 19/4/11 (Dell) 3/5/11 (Epsilon) | 27/4/11 | 12/12/11 | 20/7/11 |

959 For example, in the Telstra Bundles OMI, see Letter from Mark Hummerston, OAIC to Telstra 8 March 2012.

960 The Close Letters sent to all of the respondents were disclosed (other than the Telstra Mail Out case) however, the contents of most of these letters were heavily redacted. The Close Letters are discussed in more detail in Chapter 9.9 below.

961 Although correspondence on the investigation files indicated that draft OMI reports were sent to each of the respondents, no draft OMI report was disclosed on the basis that the drafts went to the OAIC's decision making process.

962 *Complaints Manual*, above n 227, as discussed in Chapter 7.1.1.

| | | | | | | |
|---|---|---|---|---|---|---|
| **Date response requested** | 18/11/10 | 14/1/11 | 11/5/11 | 11/5/11 | 13/1/12 | 11/8/11 |
| **Date of R's response** | 8/12/10 | 14/1/11 & 19/1/11 | 11/5/11 & 19/7/11 (Dell)<br><br>16/5/11 & 15/11/11 (Epsilon) | 11/5/11 | 3/2/12 (RFI1) and 26/3/12 (RFI2) | 11/8/11 & 21/9/11 |
| **Date Close Letter sent to R** | 16/5/11 | 10/2/11[963] | 11/1/12 | 29/6/11 | 30/4/12 | 19/12/11 |
| **Date draft OMI Sent to R** | 28/6/11 | 10/2/11 | 2/7/12 | 15/9/11 | 8/6/12 | 15/5/12 and 10/7/12[964] |
| **Date OMI report Published** | 7/7/11 | 16/2/11 | 20/7/12 | 29/9/11 | 29/6/12 | 20/7/12 |
| **Media release re OMI** | 11/10/11 | 16/2/11 | NA | 29/9/11 | 29/6/12 | 26/7/12: Letter to editor response to media |
| **Time between opening and publication of OMI report** | 11.5 months | 1 month | 15.5 months | 5 months | 6.5 months | 12 months |

*Table 5: OAIC investigation chronologies*

In most cases, the investigation concluded shortly after receipt of information from the respondent. In the 3 investigations that took close to or more than 12

963 Vodafone is the only case where the draft OMI report was sent out with the Close Letter.

964 There were two quite different OMI reports sent out in the Medvet investigation. This is discussed later.

months to complete, the greatest contributor to the delay was either the time taken to issue the Close Letter or the OMI report, rather than the investigation process itself.

In 5 of the 6 cases, the Close Letter seems to have been sent promptly following receipt of information from the respondent. The exception is the Telstra Mail Out investigation. In that case, no record of activity was disclosed for the period between 8 December 2010 when Telstra's response to the RFI Letter was received and 16 May 2011 when the Close Letter was sent. The delay in the Dell/Epsilon and Medvet investigations was due to the time taken to prepare and send the draft OMI. The Medvet investigation was completed in December 2011 at which time a Close Letter was sent that appears to find that there was no breach because no personal information had been disclosed.[965] This was presumably confirmed in the draft OMI report sent out by Mark Hummerston on 15 May 15 2012.[966] However, a further Closer Letter and draft OMI report was sent by Timothy Pilgrim in July 2012 (nearly seven months after the original Close Letter). The circumstances surrounding these reports are discussed further below, but it is worth noting the seven-month gap between the date of the first Close Letter that was sent to Medvet and the date of the final draft OMI report.

In the Dell/Epsilon investigation there was a five-month period between the Close Letters sent to Dell and Epsilon and the sending of a draft OMI report.

The delays in concluding and publishing the reports in the Telstra Mail Out and the Medvet case are concerning. Timeliness of the use of regulatory powers is one of the principles of good regulation that should guide the exercise of powers by the OAIC and which is specifically referred to in the draft *Regulatory Powers Policy*.[967]

---

965 The *Medvet Close Letter 1*, above n 928, was substantially redacted.

966 The contents of the May draft of the Medevet OMI report have been redacted in full.

967 *Regulatory Powers Policy, above n 227*, [18].

## 9.4 COMPLAINT ASSESSMENT SHEET

According to the *Complaints Manual*, an initial assessment of all complaints is made by a Director or Deputy Director to determine if the complaint should be the subject of preliminary inquiries, investigated or declined, which assessment is set out on a Complaints Assessment Sheet (CAS). Information in the CAS includes:

- Details about the complainant and respondent, including any representatives involved;
- Relevant dates, including when the letter was dated, received and assessed;
- Issues raised in the complaint; and
- Name of the industry sector to which the respondent belongs.

It also includes the issues that need to be considered before determining whether an investigation is required. CASs are given to Complaint Officers but are also reviewed by the Assistant Commissioner to 'ensure a consistent approach to decision-making and the identification of systemic issues and trends.' According to the *Manual*, the Assistant Commissioner will review the information recorded on the green sheet and, if in agreement, will co-sign the assessment.

Complaint Assessment Sheets were disclosed for all of the OMIs except Epsilon and Telstra Mail Out.[968] Those sheets that were disclosed were completed in a manner largely consistent with the process referred to in the *Complaints Manual*.

---

968 Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet, 10 January 2011 ('*Vodafone CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Vodafone 20; Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet, 27 April 2011 ('*Sony CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Sony 8; *Dell DBN CAS*, above n 895; Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet – OMI, 6 April 2011 ('*Dell OMI CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Dell 16; Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet, 12 December 2011 ('*Telstra CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Telstra 61; Office of the Australian Information Commissioner, OPC - Complaint Assessment Sheet, 19 July 2011 ('*Medvet CAS*'); attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013, schedule item: Schedule B_Medvet 23.

It does, however, appear that not all sheets had been co-signed by the Assistant Commissioner, as required by the *Complaints Manual*. The Assistant Commissioner at the time was Mark Hummerston.

| | **Vodafone** | **Dell DBN** | **Dell OMI** | **Sony** | **Telstra Bunds** | **Medvet** |
|---|---|---|---|---|---|---|
| Assessed By: | Linda | Linda | Linda | Jacob | Linda | MH[969] |
| Checked by: | - | Jacob | - | Timothy Approved | MH | - |
| Allocated to: | - | Marie | Marie | Adam | Tina | AM |

*Table 6: Complaint Assessment Sheet Review Signatures*

Details of the assessment and checking of each of the CASs are included in *Table 7*, with no indication of review for three of the five OMI files. Issues in terms of the consistency of interpretation and the application of principles that could be attributable to the Assistant Commissioner Compliance not reviewing and co-signing the Complaint Assessment Sheets are considered in Chapter 9.10.2.1.

Each of the different sheets includes notes in a section titled 'Action Officer,' which in some cases includes references to the information that the respondents should be asked to provide (which is relevant when considering the RFI Letters sent). Looking at each of the relevant sheets:

- Vodafone CAS (Case Number 14733). This case was opened as an OMI. It refers to NPP 1.3, NPP 2 and NPP 4 as the relevant principles to be considered. The notes include that the respondent should be asked to advise 'what security measures are in place to protect information R holds generally and particularly electronically.'[970]

[969] It is assumed that the initial "MH" refers to Mark Hummerston.

[970] *Vodafone CAS*, above n 968.

- Sony CAS (Case Number 15107). This case was opened as an OMI – even though there had been a data breach notification. It identifies NPP 2 and NPP 4 as the relevant principles to be considered. There may have been a separate DBN file but there is no indication of that from the documents produced. There is no reference to any particular questions to be asked of Sony.
- Dell CAS. The Dell CAS shows that that case was initially opened as a DBN case.[971] It identifies NPP 2 and NPP 4 as the relevant principles to be considered. It includes the following additional notes: 'Both Dell and Epsilon have already taken a range of actions to contain the breach … Open DBN. Write to Dell … Request a copy of incident investigation report.'[972] It is not clear what happened to the DBN file. There is a separate CAS relating to the OMI (Case Number 15073).[973] It identifies only NPP 4 (and not NPP 2) as the relevant principle for consideration. This second CAS was not checked.[974] The notes on the OMI CAS include statements referring to concerns regarding whether Dell has taken reasonable steps through its outsourcing arrangements with Epsilon. It reflects that an OMI will be opened and the Dell will be asked 'what reasonable steps' it has taken to protect personal information, what steps it has taken to ensure that third parties take reasonable steps and also includes the note 'Refer to any relevant industry standards.'[975] This is the only reference to considering standards in any of the CAS's and is considered in more detail in the next chapter. Neither CAS raised consideration of National Privacy Principle 9, the provision which applied to the cross border transfer of personal information. Dell Australia must have transferred the personal information of its Australian customers to Epsilon in some fashion, which may have raised

---

971 *Dell DBN CAS*, above n 907.

972 Ibid.

973 *Dell OMI CAS*, above n 968.

974 See Table 7 for details on which CASs had been checked.

975 *Dell OMI CAS*, above n 968.

issues regarding compliance with NPP 9. Compliance with this principle was not raised in either CAS and is not raised at any time during the investigation.

- Medvet CAS (Case Number 15394). This CAS identifies only NPP 4 as the relevant principle to be considered.[976] This is of interest because the final report finds there was a breach of both NPP 2 and NPP 4, although the initial investigation seemed only to consider NPP 4.[977] Only the front page of this document was disclosed so notes made in regard to the information to be requested were not revealed.[978]
- Telstra Bundles CAS (Case Number 15983): There is a CAS for the DBN that seems to have been opened and the transferred into an OMI file.[979] There is a second CAS for the OMI File, which includes the note 'Reports raise issues of improper disclosure and lack of reasonable steps in terms of data security measures.' There is, however, no reference to questions to be asked as part of the OMI.[980]

## 9.5 CASE PLANS

As previously discussed, one of the initial stages of any investigation should be the preparation of a case plan that identifies the relevant legal provisions and the information or evidence needed to establish whether there has been a breach of privacy, having considered the evidence to hand.[981] According to the *Complaints Manual*, case plans need to be approved by the Compliance Officer's supervisor before RFI Letters are sent.[982]

---

976 *Medvet CAS, above n 968.*

977 The Medvet decision is considered further in Chapter 8.

978 *Medvet CAS*, above n 968.

979 *Telstra CAS*, above n 968.

980 *Telstra CAS*, above n 968.

981 *Complaints Manual*, above n 227, 33. See the earlier discussion of investigation plans in Chapter 7.1.1.

982 Ibid.

No record identified as a case plan was included in any of the OMI files reviewed as part of this research.

It may be that the handwritten notes by the Action Officer included in each of the Claim Assessment Sheets represent the case plan for each OMI. If so, then it is difficult to see how they could be regarded as containing adequate or appropriate details in regard to the evidence needed to establish a breach of privacy and how that evidence is to be obtained.

The Assistant Commissioner Compliance was asked whether different investigation plans were developed for different types of breaches, for example, whether the fact that there was a malicious attack or internal accidental error influence the way the investigation was carried out.[983] Her answer indicated that these issues may only be given consideration at a very high level. While acknowledging that those issues did influence the investigation, the ACC said that that was because they raised different legislative requirements, and so different principles would need to be considered. She noted that if it were a malicious attack the OAIC would be 'looking at the NPP4 issues with great particularity, trying to ascertain the extent to which the threat could have been anticipated and mitigated against or not' rather than at NPP 2.[984] Accordingly, the direction of the investigation would seem to depend on the privacy principles that may be breached, without any more detailed consideration of the circumstances of the breach or the more particular questions that may need to be asked.

The absence of any case plan for any of the investigations suggests that no real consideration is given to issues such as the evidence that may be needed to establish breach of privacy in the particular case.

---

983 Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

984 Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

## 9.6 REQUEST FOR INFORMATION LETTERS

Because no case plan is prepared, the next step after the investigation file is opened is to send a Request for Information Letter. According to the *Complaints Manual*, the RFI Letters should:

- Outline the … allegations (of breach);
- Refer to the relevant parts of the Act (perhaps in an attachment to the letter);
- Be objective, impartial, assume nothing and by no means pre-judge the outcome of the investigation;
- Invite the respondent to provide any other information it may feel is relevant
- Inform the respondent that any information provided may be given to the complainant; and
- Give the respondent generally 21 days to respond.[985]

RFI Letters from all the investigations, other than the one sent to Epsilon, were disclosed as part of the FOI process and have been relied on for the following analysis.[986] These letters are generally consistent with the format outlined in the *Complaints Manual.* They adopt a standard format designed to meet a number of the aspects of procedural fairness referred to in Chapters 2.6.1 and 7.1.1: compliance with the fair hearing rule, which provides that the respondent should be advised of the allegations, the possible outcomes and given an opportunity to reply to the allegations; and compliance with the evidence rule, in particular the requirement that any findings be based on logically probative material. However, it is not so clear that the RFI Letters could be regarded as asking specific questions so as to obtain the evidence that the OAIC requires to support a decision on the balance of probabilities (as required by the evidence rule).

---

985 *Complaints Manual*, above n 227, Section 12 'Opening the Investigation'.

986 *Telstra Mail Out RFI Letter*, above n 802; *Vodafone RFI Letter*, above n 817; *Sony RFI Letter*, above n 829; *Dell RFI Letter*, above n 888; *Telstra Bundles RFI Letter*, above n 848; *Medvet RFI Letter*, above n 907.

All of the RFI Letters, other than the Dell Australia RFI Letter, pose a number of the same high-level questions, often in identical terms, notwithstanding the very different fact scenarios which form the basis of the different OMIs. In its RFI Letter, dated 10 January 2011, Vodafone was asked to respond to the following questions:

1. Please provide a detailed account of this incident. In your response, include details about what information, if any, was made publicly available on Vodafone's website
2. What steps, if any, has Vodafone taken or is taking in response to this incident?

…

6. Please advise what steps if any Vodafone takes to help ensure its customers' personal information is secure and is protected from loss, unauthorised access, modification and disclosure, as required by NPP4.1, including when information is held and is accessible electronically.
7. Were these steps in place and being practiced at the time of the reported incident?
8. Does Vodafone consider these steps reasonable to protect its customers' personal information from unauthorised access and disclosure? If yes, please provide details.
9. Please provide any other information relevant to the incident.

The Telstra Mail Out RFI Letter (sent shortly before the Vodafone RFI Letter) included questions identical to 6 and 7, but also asked:

- When does Telstra expect its data analysis of the incident will be complete?
- Please provide a copy of the notification letter that Telstra proposes to send to its impacted customers.

These same questions were included in the Sony and Medvet RFI Letters.

The similarity between these RFI Letters indicate that only limited consideration may have been given to the evidence required to establish the relevant facts of each case.

The incidents being investigated were very different in terms of the source of the compromise (malicious insider vs malicious external attack vs accident vs negligence), the way the compromise had been effected (unauthorised insider activity vs successful exploitation of a web application vulnerability vs human error vs technical failure), the risk profile of the organisations under consideration (large multinational organisation with 77 million users vs local mobile phone operator with much fewer users though possibly more sensitive information vs small medical testing organisation vs Australia's largest telecommunications company), the type of information compromised and the extent of and potential harm resulting from the possible breach. If consideration had been given to some of the relevant contextual issues in each case, such as the type of breach, the organisation involved and the sensitivity of the data compromised, it might be expected that different questions would be posed seeking different information relevant to the particular breach in the different RFI Letters.

By contrast, the Dell Australia and Telstra Bundles RFI Letters indicate some customisation of questions in view of the particular issues raised by those incidents, although in different ways. Dell's RFI Letter raises only two questions:

> 6. What steps does Dell Australia take to protect information it collects from customers (individuals) in order to comply with NPP 4.1?
>
> 7. Please provide details of how Dell Australia protects the personal information of its customers that it provides to third parties. Please include full details of any contractual measures in place to ensure that third parties also take reasonable steps to comply with NPP 4.1 and reference any relevant industry standards.

These questions are consistent with the notes made on the complaint assessment sheet.[987] They are also more specifically directed to the particular breach being considered than the questions posed in the other RFI Letters. However, by asking for 'full details of any contractual measures in place' and 'reference to any relevant industry standards,' the OAIC seems to be pre-empting the information it

---

987 *Dell OMI CAS*, above n 968.

wishes to receive.[988] In particular, reference to the contract suggests that the OAIC had accepted that an appropriate contract was the correct way to protect personal information transferred to a third party in these circumstances.

The fact that Dell had entered into a contract with Epsilon and was pursuing an investigation to determine whether Epsilon had complied with relevant standards (presumably in accordance with its contractual commitments) was probably communicated by Dell in its initial contact with the OAIC on 6 April 2011.[989] However communicated, this information was subsequently used to frame the RFI Letter. Taking its cue from the questions posed in the RFI Letter, Dell was able to confirm in its response that the breach had been caused by Epsilon (and attached Dell's Incident Report in that regard) and that Dell had a contract in place with Epsilon, which included a Schedule B setting out Epsilon's privacy and data obligations owed to Dell (a copy of which was attached),[990] thus satisfying the OAIC's requests for information.

Consistently with the CAS, there is no reference to NPP 9 in the Dell RFI Letter. As discussed in Chapter 9.4, it would seem that compliance with NPP 9 may have been a relevant consideration in this investigation. However, it was not raised in the Dell RFI Letter. This omission may be a result of the lack of internal review of the Dell OMI CAS.

By contrast to the very narrow request in the Dell RFI Letter, Telstra received a very broad RFI Letter as part of the Telstra Bundles OMI, asking that it respond to the following questions:

1. What is the purpose of the database and what information does it hold?
2. How did the database become publicly accessible?

---

988 Ibid.

989 Although this is not clear from the file, an internal OAIC email, 6 April 2011 refers to a phone conversation in which Dell had advised the OAIC that 'Epsilon holds customer data for Dell [words exempted on basis of s 47C and s47G FOI Act]…. Epsilon has engaged [words exempted on basis of s 47C and s47G FOI Act] to investigate the breach. … Dell indicated it would provide a final report.' It is likely that the first redaction referred to the contractual terms between the organisations. See Email thread from Delll to OAIC, 6 April 2011.

990 Letter from Dell to Mark Hummerston, OAIC, 10 May 2011.

3. How long was the database publicly accessible?
4. Exactly what information on the data was publicly accessible?
5. What kind of information features in the free-form notes field of the database?
6. How many queries were performed on the database in the time that it was publicly accessible?
7. Is there any evidence of other loss or intrusion on the database?
8. What steps has Telstra taken to contain the risks associated with the disclosure?
9. What training is available for Telstra staff with regard to the use and handling of customers' personal information, including email and internet security?
10. What steps if any does Telstra have in place with regard to data security and its website policy to protect customers' personal information from misuse loss and from unauthorised access, modification and disclosure?
11. Were these steps in place at the time of the incident? Does Telstra believe that these steps are adequate in light of its obligations under the Act?
12. If Telstra's investigation identifies a particular data security risk, does Telstra believe that its data security measures meet its obligations under the Act and that they adequately manage the risk?
13. What changes, if any, does Telstra propose to make in order to address the identified risks and satisfy its obligations under the Act?

Other than the questions directed at the database, the questions posed and the information sought in this RFI are different to those included in the RFI Letters in all the previous OMIs. It is not clear where this direction came from. No reference was

made in the relevant claims assessment sheet[991] to any specific questions to be posed as part of this investigation.

Unlike the other RFI Letters, the Telstra Mail Out RFI Letter contains a number of references to risk in questions 8, 12 and 13. This is the first time that risk has been referred to in any of the RFI Letters (although as discussed further in the next chapter, it should form the basis of any consideration of information security from an industry standard point of view). In Question 7, Telstra is asked whether there is evidence of 'other loss or intrusion on the database.' None of the other RFI Letters raise questions about other possible loss beyond that of the specific incident being investigated. It would have been interesting if this question had been asked of Vodafone, for example, as Vodafone may well have had to provide evidence of unauthorised access by other franchisees based on the published reports of 'Siebel farming.'[992] This may have led to a different conclusion in terms of breach of NPP 2 (which seems to have been decided on the basis of the single interaction between the journalist and the Vodafone franchisee that made the initial allegations about the widely available access.)

In the other investigations, a general final question is asked about providing any other information relevant to the incident. By contrast, the final question in the Telstra case asks what changes Telstra might make 'to address the identified risks and satisfy its obligations' under the *Privacy Act*. It seems to imply that Telstra will be making changes, almost assuming that current controls may not be adequate and that Telstra is in breach.

It is not clear from the investigation files how the content of the different RFI Letters was arrived at. As referred to, in 4 of the cases (Telstra Mail Out, Vodafone, Sony and Medvet), the letters seem to simply copy letters sent previously. In the Dell investigation, the RFI Letter appears to be based on the information provided by the

---

991 *Telstra Mail Out CAS*, above n 968.

992 See, eg, Asher Moses, 'Vodafone dealer shuts down after expose', *The Sydney Morning Herald* (online) 24 January 2011 <http://www.smh.com.au/technology/technology-news/vodafone-dealer-shuts-down-after-expose-20110124-1a28s.html>.

respondent itself rather than on any independent assessment of what evidence might be required to enable the OAIC to reach a decision, or the remarks included in the complaints assessment sheet.

The questions posed in each of the RFI Letters (other than to Dell) are high-level and open ended, rather than specific (as required by the *Complaints Manual*). Such questions provide the opportunity for high-level and general responses that are unlikely to support specific findings of fact. This may be appropriate where the original RFI Letters are intended as an initial investigatory step to be followed by further, more detailed questioning based on the responses received.

The Sony investigation file includes a redacted copy of a public email from Dr. Roger Clarke, a well-known Australian privacy figure, which includes a list of more specific questions that could have been asked in the Sony RFI Letter, including:

- How did the personal information come to be accessed, and in particular what vulnerability was exploited;
- What security measures had been expected to protect against that kind of attack;
- On what basis were those security measures decided upon, e.g. what form of risk assessment and risk management procedures did the company apply;
- How do the security measures that were in place line up against industry standards; and
- What further or changed measures are being applied as a result of the manifest inadequacy of the measures that were in place at the time?[993]

A copy of this email was included in the OAIC's investigation file, attached to an email chain that includes the OAIC comment 'there may be some useful comments in [redacted] questions.'[994] Dr. Clarke's comments were redacted on the basis that it was part of the OAICs decision-making process.[995] Although there were no changes

---

993 Email from Roger Clarke to privacy@lists.efa.org.au, 4 May 2011. The actual questions (or comments) made by Mr Clarke and other content of this email chain were exempted. A copy of this email is included in Appendix C ('*Roger Clarke Email'*).

994 Internal email thread, OAIC, 6 May 2011.

995 Ibid.

made to the questions in the subsequently issued Medvet RFI Letter, these comments may have influenced the longer and more detailed list of questions in the Telstra Bundles RFI Letter. However, there is nothing to indicate this connection in the files.

Dr. Clarke noted that the questions he was suggesting the Commissioner should have asked in the Sony RFI Letter may have been more appropriate for a second round of questions.[996] There is however little evidence of any 'second round' questioning in any of these investigations. Other than in the Telstra Bundles investigation,[997] there is no evidence of the OAIC looking for further detail or explanation of any of the information provided in response to the RFI Letters. In particular, it does not appear that the OAIC sought to elicit further information about how the incident occurred, the security measures that were in place, how those measures were determined to be adequate or the organisational response to the incidents in any of the OMIs following the initial RFI Letters or the receipt of investigation reports (other than Telstra Bundles).

In the Vodafone, Sony, Dell/Epsilon, Medvet and Telstra Bundles investigations, the OAIC was advised by respondents that they were conducting an investigation or had commissioned independent experts to investigate on their behalf. In each of those cases, the OAIC followed up to ensure a copy of the report from the investigation was provided to the OAIC. Investigation reports was forthcoming in most cases, other than from Dell, which is discussed further below.[998] However, there is no indication of any further questions being raised by the OAIC following receipt of these reports (other than Telstra Bundles).

One of the results of the limited follow up is that responses to the RFI Letters, together with any reports provided, comprise almost the entirety of evidence regarding the incident obtained by the OAIC and relied on in making its decisions In effect, the questions posed in the RFI Letters set the parameters for the investigation.

---

996 Roger Clarke email, above n 993.

997 Letter from Mark Hummerston to Telstra, 8 March 2012.

998 Investigation reports were provided by the respondents in the Vodafone, Sony, Dell/Epsilon, Medvet and Telstra Bundles investigations.

This makes the fact that those questions are largely generic, high level and open ended even more problematic.

An example of what this means in practice can be demonstrated by the fact that none of the questions in any of the RFI Letters are directed at identifying any systemic issues. The Epsilon records indicate that one of the questions to be raised was what other customers of Epsilon were in Australia.[999] There is no evidence that this information was sought (although the Epsilon RFI Letter has not been disclosed so it may have included this request). Similarly, there was no question raised in the Medvet investigation about the software they were using that had allowed the Google caching, including the organisation from which they procured that software or whether they knew of other users. Similarly, the report provides that Vodafone were using a Siebel database, which is the same as the database used by Telstra and which is specifically considered in the Telstra Bundles case. No questions were directed to either Vodafone or Telstra regarding their implementation of some of the specific security capabilities of the Siebel system, nor were any inquiries made about other users of Siebel systems who may have similar implementations.

Before leaving this review of the RFI Letters, it should also be noted that each RFI Letter specifically asks for information about the remediation steps taken by the organisation in response to the incident.

For example, the Medvet RFI Letter contains the following:

'2. What steps has Medvet taken, or is taking, in response to this incident?'[1000]

This is consistent with the Assistant Commissioner Compliance's statement that the RFI Letter is intended to elicit information about the remediation in addition to whether there has been a breach of the Act.[1001] The relevance of remediation steps is discussed further below in regard to the purpose of publishing OMI reports.

---

[999] *Dell DBN CAS*, above n 907.

[1000] *Medvet RFI Letter*, above n 919.

[1001] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

## 9.7 INVESTIGATION APPROACH

The next part of the process, following the sending of the RFI Letters and the receipt of responses, includes the consideration of the evidence and the determination regarding whether any additional evidence is required to support the decision-making process.

The Assistant Commissioner Compliance confirmed in the December interview that the investigation process is 'primarily a paper based investigation … in terms of asking a series of questions and then analysing the information that's returned to us.' This is consistent with the Commissioner's approach to conciliation, which is to rely on letters and phone calls and only in a 'small proportion of intractable matters' meet with the parties face-to-face.[1002]

Included in Appendix G is a table showing the different types of records disclosed from the OAIC's investigation files.[1003] This analysis supports the proposition that each investigation is conducted largely via email or letter. There are few phone calls or meetings recorded between the OAIC and the respondents. Consistent with the notion that these investigations were all conducted 'on the papers' there is no evidence of the Commissioner visiting the offices or other premises of any of the respondents or meeting with them in person, other than a visit to the Vodafone offices after the conclusion of the investigation to watch a demonstration of Vodafone's new online learning system.[1004] There is reference to a teleconference with Telstra, but that appears to have been limited to discussion of Telstra's report on the Telstra Bundles investigation, rather than separate testing of the assertions from that report. There is also reference to a teleconference with

---

1002 *Information Sheet 13*, above n 202.

1003 The data is based on the records referred to in the Resolve Action Sheet or CMS Summary Sheet for each investigation wherever available, rather than the actual records produced pursuant to the FOI requests, as those sheets were more comprehensive than the file records. Accordingly the record of activities per file will not equal the total number of records produced. There are also records that include multiple activities, for example an internal email advising of a phone call with a respondent.

1004 Internal email thread, OAIC, 7 September 2011.

Epsilon sometime in late April, but again it is unclear whether this phone conference took place.[1005]

The adoption of this 'on the papers' approach is of interest because the Commissioner has the power to 'obtain information from such persons and make such enquiries as he or she thinks fit',[1006] to require the production of 'any information or a document relevant to an investigation'[1007] and to require a person to 'attend before the Commissioner at a time and place specified in the notice to answer questions relevant to the investigation.'[1008] This applies not only to the respondents themselves but also to any third parties, who could include software developers and the providers of information technology services to any of the respondents, as well as experts (such as information security specialists) who might provide expert evidence.

According to the Commissioner those powers have been used 'frequently and for various reasons' although mostly as a consequence of the internal governance purposes of the organisations being asked to provide the information. If not statutorily required, those organisations may be in breach of other laws if they provided information without a formal statute-based request.[1009] However, there is no evidence of the use by the Commissioner of its Section 43 or 44 powers to require the production of information or to make enquiries of any persons in any of the OMI cases being considered.

In only one of the 6 cases under review was it suggested that the OAIC might use its powers pursuant to section 43 or 44. In an email exchange, the OAIC advised Telstra that if a report was not available by 30 March 2013 (Telstra having said that it would be able to report on the incident that occurred in mid-December by late January), then the Commissioner would 'issue a notice compelling Telstra to

---

1005 Email from Caren Whip to Jodie Siganto, 13 November 2013, which includes statement 'Email dated 29 April 2011 indicating teleconference did not take place', referring to an email which was not disclosed.

1006 *Privacy Act* s 43(1)(3).

1007 *Privacy Act* s 44(1).

1008 *Privacy Act* s 44(3).

1009 Interview with Timothy Pilgrim (Sydney, 14 December 2012).

respond by way of a senior executive being required to appear before the Commissioner and answer questions.'[1010]

Accordingly, it could be argued that the OAIC has underused its powers.

The Dell/Epsilon investigation provides a good example of where the Commissioner may have used its powers to secure evidence that the respondent was unwilling to provide. In that case, Dell had advised that it would undertake a security audit in response to the incident.[1011] The OAIC followed this up in July, requesting that a copy of the audit report be made available. While responding that it had 'recently completed a high-level off-site security risk assessment' and confirming that that assessment indicated that Epsilon 'met relevant industry and data security standards' and that 'data transfers were appropriate,' Dell declined to provide a copy of the report to the OAIC. The basis for so declining was that the report 'contains confidential information that relates to Epsilon's security systems that contractually Dell cannot disclose to the OAIC.' Dell further suggested that the OAIC should contact Epsilon itself because 'Epsilon will have detailed information on its own internal information security systems and procedures.'[1012]

It would seem unlikely that Dell's confidentiality obligations in its contract with Epsilon would not be subject to compliance by Dell with lawful requests by local regulators for the provision of documents or information or where required by local laws. However, there is no evidence from the investigation file that the OAIC considered issuing Dell with a request to produce the information pursuant to Section 43 or 44 of the *Privacy Act*. In fact, it does not appear that the OAIC pressed Dell for the disclosure of Dell's risk assessment in any way. It also does not appear that the Commissioner asked for or obtained a copy of Dell's assessment from Epsilon.

The Commissioner's reluctance to press Dell to produce what would have been highly relevant information is indicative of the non-adversarial approach taken by the

---

[1010] Email from OAIC to Telstra, 15 March 2012.

[1011] This is apparent from the reference to the security audit to be undertaken in the Email from OAIC to Dell, 1 July 2011.

[1012] Email from Dell to the OAIC, 19 July 2011.

Commissioner towards most of the respondents in these cases, perhaps influenced by the Commissioner's interest in arriving at an agreed resolution. This is discussed further in Chapter 9.10.2.2 below.

There is also no evidence of the Commissioner seeking evidence from third party experts (other than in those cases where third parties had input into the reports that were provided to the Commissioner by the respondents or where they had volunteered information, such as in the Medvet investigation) or from other interested parties. There is no evidence of any independent investigation by the Commissioner or verification of any of the information provided by any of the parties being investigated in any of the 6 OMIs under review.

This reliance on information provided by the respondent rather than on any independent investigation or third-party evidence gathering is supported by the OMI reports. Each report includes a statement to the effect that the information relied on by the Commissioner in forming its decision is that provided by the respondent. For example, the Dell/Epsilon report provides:

> On the basis of information received from Epsilon, the Privacy Commissioner considers that at the time of the incident Epsilon had reasonable steps in …[1013]

The Assistant Commissioner Compliance confirmed that the only area where Commission staff might actually go out to the field was in the area of audit, referring to audits as 'proactive compliance.'[1014]

As discussed in Chapter 2.6, the rules of procedural fairness include the evidence rule: there must be sufficient probative evidence that is relevant and logically capable of supporting any findings.[1015] The OAIC's willingness to form a view based on the information provided by the party being investigated with little independent verification of that information, together with the possible under-use of available powers to require production of further information, are relevant to whether

---

[1013] *Dell/Epsilon OMI Report*, above n 337.

[1014] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

[1015] *ARC Evidence Guide*, above n 238, 3. This is also required as part of the principles of good decision making referred to in Chapter 2.6.1.

the investigations could be regarded as being conducted in accordance with ideas of procedural fairness and the consequent notions of transparency, balance and vigour.

### 9.7.1 Appropriate skills

It is likely that the 'on the papers' investigation approach is a consequence of the Commission's resourcing issues both in terms of the number of available staff and the skills of those staff. When discussing the 'on the papers' approach to investigations, the Assistant Commissioner said 'one of the things that is a challenge for us is ensuring that we've got sufficient expertise to be able to analyse the information that is provided back to us particularly if it's very technical.'[1016]

In the December 2012 interview, the Commissioner acknowledged the skills issues regarding NPP 4 investigations saying:

> (this) is an area that is going to be increasingly hard for us to determine because of the nature and complexity of systems and we are already finding that. … Because as you can appreciate you need to start having some fairly well developed technical skills to be able to start assessing at a very forensic level sometimes what is going on in organisations.[1017]

Later in the same interview, when discussing the forensic skills required to carry out investigations, he said it was hard for the OAIC to attract the sort of people who had the requisite skill levels and, once in the OAIC, for those people to maintain that skill level.[1018]

Although recognising skills issues, the Commissioner does not believe this has impacted the investigation process to date. While acknowledging that the office was very reliant on the information provided by respondents and the office's internal skills, he said that he believed those skills were sufficient 'to put me in a position where I can make a sound decision on what's been presented to me.'[1019] However,

---

[1016] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

[1017] Interview with Timothy Pilgrim (Sydney, 14 December 2012).

[1018] Interview with Timothy Pilgrim (Sydney, 14 December 2012).

[1019] Interview with Timothy Pilgrim (Sydney, 14 December 2012).

there is some evidence from the investigation files that the investigators may not have sufficient technical skills.

In the Medvet investigation, two third-party reports were prepared: the first was the Deloitte report which provided an analysis of the breach and the system flaws that led to that breach occurring. A second consultant's report containing an update on the implementation of remedies to the issues raised in the Deloitte report was provided to the OAIC in late November 2011 (in response to the Commissioner's request).[1020] When considering whether to pursue a copy of this second report, an internal OAIC email states:

> Let's pursue the 2nd report then … . If the first report is highly technical it may not assist us anyway.[1021]

The implication from this email exchange is that technical reports may present difficulties to the office. It may also be that the OAIC had little understanding of the major international information security standards, ISO 27001 and ISO 27002. This is discussed further in the next chapter.[1022]

If the Commissioner's office does not have the technical skills to analyse security breaches or how they are being remediated or to assess reports providing technical details about how security breaches occurred, it is not clear how the OAIC is able to assure itself that third party expert reports are accurate, complete and based on the use of an appropriate standard of care when determining whether there has been any failure to properly protect personal information. However, this does not appear to prevent the Commissioner from foreshadowing a future reliance on third party reports.

---

[1020] All copies of these reports were redacted in full. An internal OAIC email contains the following statement '… there has been a second Consultant's Report showing what had been recommended and what has been implemented.' Internal email thread, OAIC, 9 November 2011.

[1021] Internal email from MH to LK, 10 November 2011.

[1022] See Chapter **Error! Reference source not found.**.

### 9.7.2 Reliance on third party reports

The Assistant Commissioner for Compliance, in her December interview, referred to the office's use of third party reports, calling a report on the Medvet breach 'an independent assessment of the remedial activity that had occurred' which 'the Commissioner had some regard to … in deciding whether or not it was adequate.'[1023]

However, reliance on third party reports commissioned and paid for by the organisation being investigated could raise issues of independence. At issue may be the relationship between the organisation and the third party (who may be the existing auditor or the consultancy firm responsible for prior security reviews or the implementation of security controls in the past). Also of concern could be the parameters of the review to be undertaken. A narrow scope may reduce the extent of the enquiry and result in the omission of important considerations.

Notwithstanding the ACC's approving reference to reliance on the Deloitte report in Medvet, this reliance was somewhat controversial. Questions about the Commissioner's reliance on the report, to the exclusion of its own independent investigation, were raised.[1024] In response, the Commissioner issued a letter to the editor of *The Australian* newspaper in which the inference from that article that the investigation 'was not rigorous or independent' was strongly rejected.[1025] In that letter, the Commissioner states that it 'gathered and considered information from a number of sources, including the independent forensic report completed by Deloitte's on behalf of SA Heath and information from (an) 'industry figure'.' [1026]

The role of the 'industry figure' is not clear. In the article published following the release of the OMI report, *The Australian* reported that the 'industry figure was neither interviewed nor contacted by the Privacy Commissioner in his "own motion"

---

1023 Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

1024 Hedley Thomas, '"Rigorous" probe rubber stamps audit', *The Australian* (online), 27 July 2012 <http://www.theaustralian.com.au/national-affairs/opinion/rigorous-probe-rubber-stamps-audit-praising-lab-that-broke-rules/story-e6frgd0x-1226435164479#>.

1025 Letter to the editor, above n 950.

1026 Ibid.

investigation.'[1027] This lack of contact is supported by the records from the investigation file that were made available. There is an email from an undisclosed person to the OAIC dated 19 July 2011 with the header 'C15394 – Att: Mr Timothy Pilgrim: Advice provided to Medvet in April 2011 regarding internet privacy.'[1028] An updated 'corrected' document was emailed on 20 July 2011, which was then on-forwarded within the OAIC with a message 'Hi the response from XXX.' It is not clear from the file what the email was responding to, perhaps a request for deletion of the irrelevant items. The one page attachment to both emails has been redacted in full but may have been the information provided by this third party to Medvet, which (according to the third party and the media reports at the time) Medvet failed to act on.[1029] There must presumably have been some prior contact with the OAIC because the email uses the case number that the OAIC had allotted to the Medvet investigation. However, there is nothing on the file to indicate what that prior contact may have involved.

Following these two emails, other than a file note from 27 September 2011 that could relate to a follow-up call from the industry figure,[1030] there is no record of any other contact between the OAIC and the 'industry figure' and certainly nothing to suggest that the OAIC made contact with the industry figure as part of the decision-making process.

In regard to the independence of that third party report, the Commissioner expressed the view to the researcher that he would be able to identify any lack of independence, saying 'confidently' that he would not accept a report that was not totally independent. In response to a specific question, the Commissioner confirmed that the OAIC has the skills to assess whether or not it would be appropriate to rely on a third party report.[1031] In regard to the Deloitte report relied on in the Medvet

---

1027 Ibid.

1028 Email from unknown person to the OAIC, 19 July 2011.

1029 Redactions are on the basis of *FOI Act* ss 22(1)(a)(11), 47E(d) and 47G.

1030 *Medvet Case Management Summary*, above n 918.

1031 Ibid.

report, the Commissioner appeared to consider the fact that it found a lot of failings in the system as evidence of the research's independence. The Commissioner also commented that he did not think it appropriate for the OAIC to replicate the work done by Deloitte and to 'expend the office's resources to repeat an exercise that had been done, in my view, quite independently and with a reasonable outcome.'[1032]

The commissioning of third parties to undertake investigations appears to be an attractive way forward for the Commissioner. Recently the New Zealand Privacy Commissioner has commissioned two independent reports into two major breaches affecting two New Zealand government agencies.[1033] The Australian Privacy Commissioner referred to this practice as something it would be exploring when the new powers came into force. In particular he said it would be 'encouraging' organisations and perhaps even using more formal powers to require entities to have third parties undertaken an audit, with a copy of the report to be provided to the OAIC.[1034]

The other solution to the Commission's skills issues is engaging third party experts to assist the Commission directly with its investigations. According to the Commissioner, it has already 'started to actively engage with some of those companies to see how we might be able to work together and get their services to possibly do some of that work for us through contract and the like.'[1035] However, since this interview in December 2012 there has been no public announcement or other reference to these efforts.

The other issue with third party reports is the standard used for determining whether there has been a failure to take reasonable care. In response to that query,

---

1032 Interview with Timothy Pilgrim (Sydney, 14 December 2012).

1033 Deloitte, *Ministry of Social Development - Independent Review of Information Systems Security* (November 2012) <http://www.msd.govt.nz/documents/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-deloitte.pdf>; KPMG and Information Integrity Solutions, *Independent Review of ACC's Privacy and Security of Information* (August 2012) <http://www.iispartners.com/downloads/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf>.

1034 Interview with Timothy Pilgrim (Sydney, 14 December 2012).

1035 Ibid.

the Commissioner pointed to the new *Guide to Information Security*,[1036] stating that it should be treated as 'broad guidance to organisations on what we will be looking for to determine whether an organisation has taken those reasonable steps.'[1037]

Given the gap between the industry practice and the *Guide to Information Security* (discussed previously) it may be challenging for independent information security experts to be certain about the appropriate standard to use, if retained to determine whether there has been a failure to take reasonable steps for the purposes of NPP 4.

### 9.7.3 Resources

The 'on the papers' approach to investigations, skills issues and reliance on third party reports are largely consequences of the resourcing issues facing the OAIC. The OAIC's resource issues have been recognised for some time. The ALRC referred to the significant expansion of the responsibilities of the OAIC, which 'resulted in more functions and powers for the Commissioner, although not always a commensurate increase in resources.'[1038] In the last 12 months, the OAIC's resource issues have been exacerbated by the 'daunting task' of developing guidance to assist with the new APPs 'given that it has received no additional resourcing for this implementation work.'[1039]

More recently, the Privacy Commissioner has been public about the resource pressures facing the office, with staffing numbers decreasing 'in line with the [office's] need to meet efficiency dividends imposed by government.'[1040] One of the most obvious consequences of this is the long waiting period before a privacy complaint is allocated to an investigating officer: it is presently taking about 19

---

1036 *Guide to Information Security*, above n 63.

1037 Ibid.

1038 *For your information,* above n 32, [45.2].

1039 *2013 OAIC Annual Report*, above n 381, Statement from Privacy Commissioner, xiv.

1040 Ben Grubb, 'Long delays before privacy complaints assessed', *The Sydney Morning Herald* (online), 12 September 2013 <http://www.smh.com.au/digital-life/consumer-security/long-delays-before-privacy-complaints-assessed-20130912-2tn72.html#ixzz2yY0zIYho>.

weeks longer than the usual four-week period.[1041] This raises issues in regard to the timeliness of investigations, which is one of the aspects of procedural fairness.[1042]

In response to the decrease in staffing levels, the OAIC undertook an organisational restructuring, which aimed to deliver 'greater efficiencies in a constrained budgetary environment.'[1043] This involved a move to integrated branches, each of which undertake work in relation to the OAIC's three functions of information policy, privacy and FOI. According to the *2013 Annual Report*, this integrated structure 'offers flexibility in resource allocation, provides staff the opportunity to grow knowledge and skills, and enables the OAIC to find efficiencies through maximising use of skill-sets, prioritisation and work allocation.'[1044] The 'Dispute Resolution' branch now carries out investigations in relation to compliance with the *Privacy Act* and the *Freedom of Information Act*. Own motion investigations and audits are conducted by the 'Regulation and Strategy' group, which also provides advice and guidance about the *Privacy Act* and the *FOI Act*.[1045] It is not clear why complaint-based and Commissioner-initiated investigation should be handled by different sections of the OAIC, how this restructure will support greater efficiencies or what the effect may be on the resourcing and skills issues facing the Privacy Commissioner. It may be that these issues become more acute by this reorganisation, where the same staff will be investigating both FOI and privacy compliance issues.

The dilution of expertise caused by the reorganisation may also be exacerbated by the real reduction in the number of staff available to undertake investigations. The staffing estimate for the OAIC when it was first established was for approximately 100 staff to carry out the FOI, privacy and information policy functions.[1046] As of 3

---

1041 Ibid.

1042 See the earlier discussion in Chapter 2.6.

1043 Ibid.

1044 Ibid.

1045 *OAIC 2013 Annual Report,* above n 381, 11 – 12; and Office of the Australian Information Commissioner, *Our Structure* (March 2013) < http://www.oaic.gov.au/about-us/who-we-are/our-structure/>

1046 *OAIC 2013 Annual Report*, above n 381, 5.

July 2013 there were the equivalent of 74.23 full-time staff, 25.78 of whom worked in the dispute resolution branch (covering both FOI and privacy-related complaints).[1047]

The resource issues of the OAIC are not unique. Information commissioners around the world face serious budgetary constraints and expect higher workloads, according to a survey of commissioners, which found that 77% believe that their financial and staff resources, are 'insufficient'(58%) or 'not at all sufficient' (19%).'[1048]

The UK ICO, which has a similar remit to the Australian Privacy Commissioner, has recently issued a consultation document to assist in the consideration of ways that the office may restructure itself. The document identifies a 'series of challenges under three main headings':

- The growing importance of information rights;
- Reduction in funding; and
- Major changes to the regulatory landscape (with the expected introduction of the new Data Protection Regulation).[1049]

Similar challenges face the OAIC.

Solutions being considered by the ICO include changing how it handles casework and enquiries to allow it to identify and address wider compliance issues, and only where appropriate to address individual concerns, in addition to increased coordination with other organisations and regulators.[1050]

The Canadian Information Commissioner recently reported that the effect of budget cuts on the operations of its office 'puts us at the limit of our financial and

---

[1047] Grubb, above n 1034.

[1048] Centre for Freedom of Information, *Commissioners Report Low Budgets, Growing Workloads* (12 April 2013) <http://www.freedominfo.org/2013/04/commissioners-report-low-budgets-growing-workloads>.

[1049] Information Commissioner's Office, *Looking Ahead Staying Ahead: Towards a 2020 Vision for Information Rights* <http://www.ico.org.uk/about_us/consultations/our_consultations>.

[1050] Ibid.

organizational flexibility.'[1051] According to reports, staff reductions in the Canadian Information Commissioner's office meant that Departments 'lost institutional memory with the departure of senior officials … and document-filing systems suffered with the loss of clerical staff.[1052] The same would appear to be happening to the OAIC based on the issues raised during the course of responding to the FOI submitted as part of this research.[1053]

In a recent Senates Estimates Hearing, the Australian Information Commissioner was asked directly whether the OAIC's work is being compromised because of the lack of resources.[1054] The Commissioner responded: 'We do not think the quality of the work has been compromised. The way we have put it is that we are unable to meet the performance standards that we set for ourselves.'[1055]

It is difficult to see how the Australian Information Commissioner can make that assertion given that this research has identified that resourcing issues have contributed to:

- The lack of timeliness and completeness of responses to FOI requests;
- A decline in the number of audits undertaken;
- A decline in the publication of case notes;

---

[1051] Office of the Information Commissioner Canada, *Ensuring operational integrity and corporate support for investigations* < http://www.oic-ci.gc.ca/eng/annual-reports-rapports-annuel_2012-2013_9.aspx>

[1052] Dean Beeby, 'Budget cuts undermine federal access-to-information system: watchdog', *The Canadian Press* (online), 7 April 2013 <http://www.ctvnews.ca/politics/budget-cuts-undermine-federal-access-to-information-system-watchdog-1.1227794>.

[1053] See the discussion of the OAIC's response to the FOI requests made as part of this research in Chapter 4.3.2.

[1054] Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing Budget Supplementary* (18 November 2013), 63 - 65 . In the Senate Committee Hearings the previous year, the Privacy Commissioner had said that he considered that the OAIC's level of activity in all areas of its compliance work, complaints and national investigations, would be impacted on obviously by the number of resources the office had and that there was potential for the Office's ability to respond to high profile data breach cases to be impacted; see Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing* (14 February, 2012), 41 – 43.

[1055] Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing Budget Supplementary* (18 November 2013), 64.

- A decline in the number of OMIs undertaken;
- A decline in the number of OMI reports published;
- Delays in assigning new complaints to a handling officer, which are close to five months, or five times longer than the preferred period;
- The conduct of own motion investigations via an 'on the papers' approach, a less rigorous method than a full investigation; and
- Issues regarding the office's ability to retain staff with the appropriate skills to carry out complex investigations in data breach cases.

## 9.8 DECISION-MAKING

The investigation files provide very little evidence regarding how the OAIC arrived at a decision as to whether there has been an interference with privacy in the 6 cases under review. This is not surprising given that one of the main grounds for redaction of records was that they related to the OAIC's decision-making process.[1056] This extended to all draft OMI reports as well as to most of the substantive parts of the Close Letters sent to the different respondents. Broadly, any record that might have provided any information relevant to decision-making was redacted.

Review of the summary sheets for each of the investigations files included in the disclosed records, which sheets list all of the actions that took place in each investigation, does not throw any light on the process that may have been used to arrive at a decision in a particular case.[1057] For instance, there is no reference to any internal meetings to determine outcomes or briefing notes being drafted or sent to case supervisors for consideration and decision on outcomes.

Although the files do not reveal the process by which decisions were made in any of the investigations, they do indicate that in most cases the decision regarding whether there has been an interference with privacy was arrived at quite quickly. In

---

[1056] See the reasons provided for redacting records, discussed in more detail in Chapter 4.3.2.

[1057] See, eg, *Sony Case Management Summary Sheet*, above n 843; *Medvet Case Management Summary*, above n 918.

the Sony investigation for example, a file note records that, at an internal OAIC meeting occurring the day after Sony's response to the RFI Letter was received by the OAIC, it was agreed that there was no breach. Similarly, there is a note from the case officer in the Medvet investigation file dated 11 October 2011 that states '… we received a response from Medvet on 21 September and I have assessed the response and it appears that R has taken reasonable steps and we are in a position to finalise.'

It may be that there is no consistent process for decision-making as part of the own motion investigations. This proposition is supported by the decision in Medvet. The facts of that investigation have been included in Chapter 8.1.6. To recap, following receipt by the OAIC of two external reports (one about the incident and the other about the remediation steps) a Close Letter was sent to Medvet on 19 December, 2011.[1058] That letter advised that Medvet was found to be in breach of NPP 4 but not in breach of NPP 2.[1059] From the files, it is not clear how that decision had been reached. The file note made following receipt of the Deloitte investigation report (which report was heavily relied on to establish failure to take reasonable steps in the OMI report) states that the investigating officer had assessed Medvet's response (which included the Deloitte report) and found that 'it appears that R has taken reasonable steps and we are in a position to finalise.'[1060] There is no reference to any new evidence, other than the report on the implementation of the remediation steps, being received after that time or further internal meetings being held to discuss the case. Nearly seven months after that Close Letter, in July 2012, a new Close Letter was sent to Medvet that advised of a new finding of breach of NPP 2 (in addition to the previous finding of breach of NPP 4).[1061] The basis for this change to the previously communicated findings is difficult to understand. It may be that the different decision was due to an alternative view being taken of the facts by the Commissioner, who, according to the new Close Letter, conducted a review of the

---

1058 *Medvet Close Leter 1*, above n 928.

1059 Ibid.

1060 OAIC, File note, 11 October 2011; referred to in *Medvet Case Management Summary*, above n 920.

1061 *Medvet Close Letter 2*, above n 929.

file as part of finalising the draft OMI report.[1062] Because almost the entirety of this letter had been redacted, it is difficult to determine the basis on which the Commissioner determined that there had been a breach of NPP 2, and how that varied from the reasoning used to arrive at the earlier and opposite conclusion.

The fact that the Commissioner felt it appropriate to change the communicated findings of an investigation may suggest a problem with the decision-making process.

Problems with the decision-making process may be a consequence of the OAIC's own approach to decisions. If cogent and comprehensive reasons are not provided for decisions made about the application of the NPPs to different fact situations considered by the OAIC, it makes it more difficult for the OAIC itself, as well as the regulated community to assess how those NPPs might be interpreted and applied in different fact situations. A document forming part of the Dell investigation file indicates that the OAIC itself may have been concerned regarding how to reconcile its findings in regard to NPP 2 and NPP 4.[1063] This is discussed further in Chapter 9.10.2.1.

One other aspect of the decision-making process is clear from the investigations and published reports. In these investigations, the OAIC is interested in reaching an agreement with the respondent as to the remediation of any issues. Specific references in the different reports to the agreed remediation of issues is discussed in Chapter 9.10.2.2. This focus on being able to cite agreed outcomes from the investigations in the published OMI reports is akin to the conciliatory approach used to resolve complaint-based investigations (and discussed in Chapter 7.1.2 and 7.1.3 above). There is support for the proposition that in OMIs the Commissioner is seeking to arrive at an agreed solution with the respondents. The Australian government noted that OMIs should have a similar enforcement regime as for complaints and that, in line with current processes, the Commissioner would

---

1062 *Medvet Close Letter 2*, above n 929.

1063 Internal email from NR to KO, 24 May 2012 ('*NPP 2 and NPP 4 Email*'). All of the header and footer of the document have been redacted so there is no context for the content. A copy of the 1 page untitled email excerpt is included in Appendix C.

continue to seek to settle own motion investigations via conciliation and only proceed to a determination where a settlement is unable to be facilitated or is inappropriate.[1064] The OAIC's preference for working with the respondent was confirmed in the researcher's interview with the Assistant Commissioner Compliance. After noting the difficulty with OMIs caused by the current lack of enforcement powers, the ACC said that in conducting OMIs the OAIC seeks to arrive at agreed remediation steps: although not conciliations, because they only involve one party, they are 'still about trying to influence and bring to some consensus or resolution.'[1065] It is likely that the focus on agreed outcomes to OMIs is a consequence of the limited powers available to the Commissioner regarding own motion investigations.[1066] However, the effect of this approach on the investigative process should be noted. Investigations focused on reaching agreement with the respondent as to the outcomes may involve a different approach to those investigations conducted with a view to determining whether there has been a breach of the Act. The *Complaints Manual* notes the different skills that are required of investigators depending on whether a conciliation or an investigation is being pursued, suggesting that where a conciliated outcome is the focus, less weight is placed on the formal investigation.[1067] This in turn has implications for the published investigation report. Reports based on negotiated outcomes with the respondents may not be based on vigorous investigations directed at determining whether there has been a breach of the Act and may not provide the transparency of decision-making that might be expected in a more contested case. The analysis of the 6 investigations supports the view that those investigations have been less than rigorous and that the OAIC has been concerned to reach some consensus with the respondents. This in turn suggests that the value of those reports as general guidance

---

[1064] Australian Government, above n 805.

[1065] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

[1066] Limitation of the actions available to the Commissioner following the completion of an OMI has been discussed in Chapter 7.2.3 above.

[1067] See Chapter 7.1.1.

is diminished, representing conciliated outcomes rather than decisions based on the outcome of vigorous investigations.

## 9.9 CLOSE LETTERS

Once an investigation is complete, the Commissioner issues a letter (called a 'Close Letter' in this research).

The Close Letter is drafted to comply with the OAIC's interpretation of 'procedural fairness' as contained in the *Complaints Manual* and the right to a fair hearing as part of the generally accepted ideas of procedural fairness discussed in Chapter 2.6.1. According to these principles, the OAIC must take steps to advise entities being investigated of three pieces of information before closing an investigation:

- First, that it proposes to close the complaint;
- Second, why it intends to close the complaint; and
- Third, that it is offering the complainant a reasonable opportunity to make a submission before it closes the complaint.[1068]

Close Letters were disclosed for all of the OMIs except Epsilon.[1069] Each of these Close Letters follow a similar format and generally comply with the above requirements, although large sections of all the Close Letters, other than the Telstra Mail Out Close Letter, have been significantly redacted on the basis that the contents went to the OAIC's decision-making process or contained confidential information of the respondent.

On receipt of the Close Letter in the Telstra Mail Out investigation, Telstra argued that it had not been provided with a right to be heard with respect to the application of the privacy principles, in particular NPP 2. Telstra proposed that the

---

1068 *Complaints Manual*, above n 227, 14.

1069 *Dell Close Letter*, above n 907; *Medvet Close Letter 1*, above n 928; *Medvet Close Letter 2*, above n 929, *Telstra Mail Out Close Letter*, above n 807; Letter from Timothy Pilgrim to Vodafone, 16 February 2011 ('*Vodafone Close Letter*'); *Sony Close Letter,* above n 832; T*elstra Bundles Close Letter*, above n 866.

matter of its right to be heard would be the subject of separate correspondence.[1070] However, there is no record of any separate communication between Telstra and the OAIC in regard to this point and it is not clear how the issue was resolved. The opportunity to make submissions forms part of the right of the respondent to be heard. Ensuring that parties have a right to be heard is part of the OAIC's commitment to undertake its investigations in accordance with the principles of procedural fairness.[1071] Telstra was the only respondent to raise issues in regard to its right to be heard.

The only Close Letter which is problematic is that sent to Medvet, because of the change in findings and the issuing of a second Close Letter, as discussed in the previous section. The second Close Letter included a new draft OMI report. Medvet was given only ten days to respond to the new draft OMI report before it was to be published, which arguably may not have been sufficient time in all the circumstances.[1072]

Generally, there seems to have been little disagreement by the respondents in the cases under consideration in regard to the way that the Close Letters and OMI reports describe the OAIC's findings in regard to NPP 4. More controversial have been questions of whether the OAIC has jurisdiction under the *Privacy Act* (raised in Sony) or the operation of NPP 2 (raised in Telstra Mail Out), neither of which issues are of relevance to this research.

## 9.10 OMI REPORTS

All draft OMI reports were fully redacted on the basis that they went to the OAIC's decision-making processes. Accordingly, it is difficult to determine any negotiated changes from the initial draft OMI reports sent out by the OAIC and the reports as finally published. However, some comparison can be made between the

---

[1070] Email from Helen Lewin, Telstra to Timothy Pilgrim, OAIC, 26 May 2011, which provides that 'Telstra would like an opportunity to be heard' in regard to the application of NPP 2, continuing 'We will write separately in relation to this.'

[1071] The principles of procedural fairness as they have been interpreted by the OAIC have been discussed in Chapter 2.

[1072] *Medvet Close Letter 2*, above n 929.

final published OMI reports and those parts of the Close Letters made available for each of the investigations. Generally, other than Medvet, the findings in the Close Letter seem consistent with the findings in the published OMI reports.

The relationship between the Close Letter and the OMI report is different in each investigation. For example, in Vodafone, the Close Letter and OMI report were agreed between the OAIC and Vodafone at the same time,[1073] as also seemed to be the case in Sony.[1074] In the Telstra Mail Out case there was a six-week gap between the Close Letter and the OMI report.[1075] There was a longer delay in Dell/Epsilon, but it was not so problematic in that case because there was no finding of breach. There was also a delay between the Close Letter and the OMI report in Medvet's case, in addition to the change in position between draft OMI reports.

It is not clear in these cases whether, at the time that the OAIC sent out the Close Letter, the respondent was aware that the OAIC intended to publish a report, or in fact whether the OAIC itself had formed a view on publication. Close Letters, which included findings of breach in the Vodafone, Medvet and both the Telstra cases, might have been viewed differently by the respondent if they knew that those findings would be publicly released. A file note included in the Sony file confirms that the respondent was advised very early in the investigation that, given that the Sony breach was in the public domain, the Commissioner would like to make a statement about the findings once the investigation was completed. The note also confirms that the OAIC would liaise with Sony to ensure that no commercially sensitive information would be published.[1076]

Given that such a small proportion of OMIs are the subject of public reports, it might be appropriate that the Close Letters inform the respondent of the intention to publish the result of its investigation, assuming that the respondents had not been so

---

[1073] See, eg, Letter from Timothy Pilgrim, Privacy Commissioner to CEO Vodafone, 16 February 2011.

[1074] Email from OAIC to Sony, 29 June 2011.

[1075] See Chapter 9.3 for detail on the chronology of each investigation.

[1076] OAIC, File note, 3 May 2011. See also, Internal email thread, OAIC, including email dated 24 May 2011; which states: 'spoke to [redacted] yesterday. I confirmed we would be making a media statement accompanied by a short report upon closing the investigation.'

previously advised. Respondents are given the opportunity for input into the OMI report but this may be of little value if they have accepted the findings in the Closed Letter without any expectation that those findings would be made public.

The format of the OMI reports and the change in format from February 2011 with the publication of the *Vodafone OMI Report* has already been discussed.[1077]

### 9.10.1 Decision to Publish OMI report

As discussed, the *Guide to Producing Case Notes* sets out a process for the selection of cases from which to publish a case note that involves a case officer flagging potential cases for publication of case notes, which are then given further consideration by the case note Project Manager and consultation with Compliance where appropriate.[1078] The same process applies to the publication of reports of OMIs.[1079]

According to the Assistant Commissioner Compliance, the practice is that the case officer writes the first draft of the report, which then goes through a clearance process which includes the Deputy Director, Compliance, the Director, Compliance and then to the Director of Policy who would have 'input into, for instance, is the report structured in the right way to be a good educative tool of precedent value, that sort of thing.' It also goes to the Corporate and Public Affairs team to consider 'media messaging and how that might occur' and then to the ACC and finally to the Privacy Commissioner.[1080] The ACC did not indicate who made the initial decision on whether to publish a report.

A review of the files of the 6 OMIs under review indicates that the preparation process outlined by the ACC is followed. However, it is not so clear that the Guide's process for the selection of case for reporting has been followed.

---

[1077] See Chapter 7.1.4.

[1078] *Guide to producing case notes*, above n 248, Selecting a suitable case for a case note.

[1079] Ibid.

[1080] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

The files for the OMIs under review indicate that the Deputy Commissioner for Compliance and the Privacy Commissioner personally played a significant role in determining whether a report on an OMI should be published, reviewing the proposed OMI reports and negotiating their terms with the respondent in at least 5 of the 6 investigations. The Privacy Commissioner seems to have been particularly active in decision-making around whether a report should be published.[1081] As an example, a note in the Medvet file records:

> Discussed possibility of report with MH. … MH said we will wait for TP [22(1)(a)(ii) exemption] to see if he wants to issue public report.[1082]

The Sony investigation files indicate that although most of the communication was handled by Linda King, then Acting Director Compliance for the OAIC, Timothy Pilgrim was involved in settling the final Close Letter and attached OMI report.[1083] The OAIC email, sending a draft of Close Letter and the OMI report to Sony, refers to the Commissioner's clearance being obtained to sending out those documents.[1084]

In the Telstra Bundles case the Close Letter was sent out after the Commissioner 'made minor changes'[1085] and the OMI report (having been reviewed by Policy)[1086] was sent out under cover of a letter signed by Mark Hummerston, the then-Deputy Commissioner Compliance.[1087]

Timothy Pilgrim's involvement in the decisions to publish some of the own motion investigations was also confirmed in the interview with the Assistant Commissioner Compliance.[1088]

---

1081 See Chapter 8:

1082 OAIC, File note, 19 December 2011.

1083 See email from Timothy Pilgrim to Linda King, 24 May 2011.

1084 Email from Linda King to Sony, 29 June 2011.

1085 OAIC, File note, 30 April 2012.

1086 OAIC, File note, 9 May 2012.

1087 Letter from Mark Hummerston, OAIC to Telstra, 8 June 2012.

1088 Ibid.

In addition to its involvement in determining whether or not to publish a report, the Commissioner was also active in deciding to name the organisation in published OMI reports, which was a significant departure from previous practice. The Telstra Mail Out case, which was one of the first OMIs where it was proposed to publish a report naming the respondent, supports this. Correspondence from that investigation indicates that Telstra was very concerned about the publication of the report, particularly the inclusion of the Commissioner's findings that there had been a breach of NPP 2.1. In an email exchange occurring after the Close Letter had been sent by Mark Hummerston to Telstra, Timothy Pilgrim himself reassured Telstra, confirming that there would be further discussions before the publication of a report.[1089]

The only investigation where there is little evidence of the Commissioner's involvement regarding the decision to publish a report is the Dell/Epsilon investigation, where there are few records relating to the preparation of the OMI report at all. The resolve reports for both the Dell and Epsilon files show no activity on either file between the issuing of the Close Letters on 11 January 2012 and the sending of the draft OMI report to both Dell and Epsilon for comment on 3 July 2012.

Based on the above, it seems fair to assume that the current Privacy Commissioner has been at the very least instrumental in, if not ultimately responsible for, determining whether an OMI report should be published in regard to an investigation and whether the respondent organisation should be named. This would suggest that the Privacy Commissioner had some particular purpose to achieve from the publication of these reports.

### 9.10.2 Purpose of publishing OMI reports

The general reasons given for publishing case notes and OMI reports have been discussed previously.[1090] The main three reasons are:

- To provide transparency of decision-making;

---

[1089] Email from Timothy Pilgrim, OAIC to Helen Lewin, Telstra, 27 May 2011.

[1090] See Chapters 6.4.1 and 7.1.4.

- To provide transparency of compliance activity; and
- To act as a deterrent.[1091]

#### 9.10.2.1 Transparency of decision-making

Transparency of decision-making, in terms of providing adequate reasons to support the decision as part of procedural fairness, has been discussed in Chapter 2.6.1. In that chapter it was proposed that, to be considered as transparent in this sense, each OMI report should clearly state:

- The decision;
- The findings on material facts;
- The evidence or other material on which those findings are based; and
- The reasons for the decision.[1092]

In addition to the general statements regarding the publication of case notes and OMI reports to provide transparency of decision-making,[1093] the OAIC's response to the researcher's request for access to records in regard to these 6 investigations asserted that the OMI reports provided transparency of decision-making. [1094] Accordingly, it would be expected that the 6 OMI reports considered here would meet the above criteria for transparency.

Generally, there is much in each of the OMI reports that could be regarded as educative; however, it is not so clear that any of the reports meet all of the above requirements in terms of providing sufficient reasons so as to provide real transparency of decision-making. All of the reports are clear in terms of the decision on whether there has been any interference with a privacy principle, with appropriate

---

1091 Ibid.

1092 *ARC Decision Guide*, above n 242, 7. The sufficiency of the evidence relied on and the connection of the evidence to the findings of material fact and the decisions in each case is considered elsewhere in this research.See Chapters 9.7, **Error! Reference source not found.** and 10.1

1093 Transparency of decision making and its links to procedural fairness and the provision of reasons for a decision have been discussed in Chapter 2.6 above.

1094 See the discussion of the FOI request in Chapter 4.3.2 above.

references to the legislation and the relevant privacy principles. This is a significant and important departure from the earlier OMI reports, which contained few findings of breach, and often relied on post-incident remediation in reaching a decision.[1095] All of the reports also include a statement which could be regarded as a statement of findings in regard to the material facts (which support whether there has been an interference with privacy).

Where the reports are not so clear is in detailing 'all the steps in the reasoning process that led to the decision, linking the facts to the decision' in a way that would enable a reader to understand exactly how the decision was reached.[1096] This is best illustrated by detailed reference to each of the OMI reports, other than the *Vodafone OMI Report*, which is the only case out of the 6 where clear and adequate reasons for the decision is made by reference to relevant findings of fact. The Vodafone decision is considered in more detail in the next chapter.

The *Telstra Mail Out Report* identifies the security measures that were in place (as advised by Telstra), which findings are used to support the conclusion that this was a case of one-off human error, rather than a failure to take reasonable steps. The adequacy of this reasoning is discussed further in the next chapter. In the decision, it is also decided that the disclosure of a person's name by itself is an unauthorised disclosure of personal information for the purposes of NPP 2. This is a very important example of the Commissioner's interpretation of 'personal information.' However, the OMI report only devotes two sentences to the issue:

> The incorrectly addressed letters sent out by Telstra included the names and telephone details of individuals. In the OAIC's view, a person's name is 'personal information' and does not have to be linked with other information to fall within the definition of personal information set out in the Act.[1097]

There is no reference to any principle, guidance or previous case to support what it states to be 'the OAIC's view.' The Commissioner must have been aware that this

---

[1095] See Chapter 6.4 above.

[1096] *ARC Decision Guide*, above n 242, 8.

[1097] *Telstra Mail Out OMI Report*, above n 334.

interpretation of 'personal information' was in some way novel because Telstra had taken particular issue with it in correspondence with the OAIC.[1098] However, it is difficult to regard the two sentences in the report as providing 'all the steps in the reasoning process' that led to the Commissioner's finding

In contrast, two full paragraphs in the conclusion of the report are devoted to Telstra's response to the incident, referring to the way that Telstra 'acted promptly to prevent further breaches' and 'helped to ensure that the breach was contained and no further unauthorised disclosures occurred.' The report also notes with approval that Telstra had notified the affected customers, giving those individuals 'an opportunity to take appropriate action, if necessary, to mitigate any harm they may suffer.'[1099]

In both the Sony and Dell/Epsilon investigations, the findings of a sophisticated cyber-attack seem to be sufficient explanation for the loss of data without a more detailed consideration of the attacks themselves, including the vulnerabilities successfully exploited and whether those vulnerabilities would have been existed if reasonable security steps had been taken. As is discussed in the next chapter, none of the security measures referred to in either report are particularly relevant to the actual security compromise in each case, so their inclusion is somewhat confusing, and the consequential finding that reasonable steps had been taken is not compelling.[1100]

More importantly, in terms of interpretation of the privacy principles, the *Sony OMI Report* supports the view that where information is accessed by an unauthorised malicious third party (in this case the on-line activist group Anonymous) there is no 'disclosure' for the purposes of NPP 2. However, little detailed reasoning is provided to support this interpretation. The relevant part of the OMI report is as follows:

---

[1098] Email chain between Linda King, OAIC and Helen Lewin, Telstra, 28 June 2011.

[1099] *Telstra Mail Out OMI Report*, above n 334.

[1100] See also Bloom and Frketic, above n 55, which refers to the OAIC's reasons in Sony as 'broad brush and cursory.'

> In general terms an organisation discloses personal information when it releases information to others outside the organisation.[3]
>
> Media reports of this incident claimed that customer information, including personal information was disclosed to a third party. However, this was not substantiated by any of the evidence provided to the OAIC. The evidence showed that no personal information was disclosed to unauthorised parties; rather the information was accessed as a result of a sophisticated security cyber-attack against the Network Platform.[1101]

The footnoted reference is to the OAIC's *Guidelines to the National Privacy Principles*, which includes a definition of 'disclose' in exactly the terms quoted.

In discussions with the Assistant Commissioner Compliance the researcher queried how 'disclose' had been interpreted and applied by the OAIC in the recent cases. The ACC referred to the Sony case as being the precedent for the interpretation of 'disclosure' as meaning the 'release' of information in a positive sense, rather than the accessing of information as a result of a sophisticated cyber-attack, without any positive act by the respondent. When the researcher queried whether the malicious attack was the key regarding whether there was a disclosure, the ACC replied that 'the external access … means that the organisation itself didn't do something to release the information.'[1102] The OAIC's failure in the report to explicitly build on the word 'release' as part of the definition of 'disclosure' by referring to the need for some sort of positive act by the entity detracts from the transparency of the decision-making.

The decision in regard to 'disclosure' and cyber-attacks in the *Sony OMI Report* may explain why the question of whether there was any unauthorised disclosure pursuant to NPP 2 was not raised in the *Dell/Epsilon OMI Report*. The report is silent on the application of NPP 2 to the circumstances. The failure to consider NPP 2 may also be a consequence of reference to NPP 2 being omitted from

---

[1101] *Sony OMI Report*, above n 335.

[1102] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

the Dell OMI CAS which was not reviewed in accordance with the OAIC's process.[1103]

There is some suggestion that the OAIC recognised this oversight and considered correcting the report. An email already referred queried whether the NPP 2 issue had been inserted into the Dell case 'or was it decided not to as the close letters had gone out?'[1104] As the final OMI report does not include any consideration of NPP 2, the decision must have been made not to amend the OMI report.

Leaving aside the omission of reference to NPP 2, it is difficult to determine what the intended educative purpose from publication of the Dell/Epsilon report might have been. It deals very briefly with the issue of the contractual terms between Dell and Epsilon, a current and highly topical issue for many organisations that are considering outsourcing or cloud computing arrangements which involve the disclosure of personal information. In this case, the report states that the Commissioner found that:

> by entering into the contractual agreement with Epsilon, Dell Australia had reasonable steps in place to protect the personal information it holds from misuse and loss and had met its obligations under NPP 4.[1105]

This statement provides little information in terms of transparency of decision-making. It does not provide any detailed consideration of the type of contractual provisions that the Commissioner would consider as satisfactory for Dell to meet its obligations to take reasonable steps pursuant to NPP 4. Dell's response to the Commissioner's RFI Letter included a statement to the effect that because Epsilon 'is a multinational company of high regard who provide similar services to an extensive client base' it was reasonable for Dell to assume that Epsilon 'would have appropriate measures in place to safeguard Dell's subscriber information in a manner consistent with Epsilon's contractual obligations to do so'[1106] - a proposition that the

---

1103 *Dell OMI CAS*, above n 909. See the discussion in Chapter 9.4 above.

1104 *NPP 2 and NPP 4 Email*, above n 1063.

1105 *Dell/Epsilon OMI Report*, above n 337.

1106 Letter from Dell to Mark Hummerston, OAIC, 10 May 2011.

Commissioner appears to accept. It also skirts the issue of whether Dell had any ongoing obligation to ensure that Epsilon had implemented and was maintaining security measures in accordance with those contractual obligations. By providing that Dell had taken reasonable steps 'by entering into the contractual agreement' the Commissioner seems to absolve Dell from any oversight obligation regarding the discharge by Epsilon of its contractual duties. This does not seem to be an appropriate finding, particularly in view of the subsequent Telstra decision where failure to ensure that processes (which could be equated to contracted obligations) were being followed meant that Telstra was found to be in breach.

The issues in relation to the application of the *Privacy Act* to the Sony entities involved in the breach and to Epsilon as a US incorporated entity, and whether any of those international entities could be regarded as carrying on business, were referred to but without any attempt to resolve them. In both cases, the fact that there was no breach meant that the Commissioner did not have to form a view about the application of the Act to the non-Australian incorporated entities.

The *Medvet OMI Report* is perhaps the least compelling in terms of the transparency of decision-making. Issues in terms of the interpretation and application of NPP 4 are examined in the next chapter. However, the reasoning in the report to support the finding that there had been an unauthorised disclosure for the purposes of NPP 2 is worth further examination. After repeating the same single statement of principle contained in the Sony report, that is, that a disclosure involves the release of personal information, two significant findings are made in a single sentence:

> After reviewing the Deloitte report and other information provided by Medvet, the Commissioner formed the view that having regard to the nature of Medvet's business, including that its customers were individuals as well as commercial entities, that the accessibility of address information on the internet constitutes unlawful disclosure of personal information.[1107]

Breaking this down, the Commissioner found that:

---

[1107] *Medvet OMI report*, above n 338.

- In the circumstances, the address information by itself was 'personal information;' and
- The availability of that address information on the internet was a 'disclosure.'

The second finding in particular represents a fairly significant departure from the reasoning used in Sony, as explained in the interview with the Assistant Commissioner, that there needs to be some positive act of release by the respondent for there to be a disclosure. However, the single paragraph sheds little light on the reasoning the Commissioner used to arrive at either of these findings.

That compliance with NPP 2 was a difficult issue in the circumstances, and perhaps deserving of greater discussion in the OMI report, is demonstrated by the fact that the OAIC's own view changed between the issuing of the Close Letter in December 2011 and the draft OMI report sent in May 2012, and the updated OMI report sent in July 2012 following the Commissioner's internal review of the file. From a document on the Dell file, it is clear that in May 2012 it was the OAIC's view that Medvet 'had caused information to be available on the internet however there was insufficient evidence to show the disclosure of personal information, so no breach of NPP 2'[1108] However, at some time between 22 May 2012 and July 2012, the Commissioner reached a different decision, as evidenced by the finding in the published OMI report, and as communicated in the second close letter sent in July.[1109] In these circumstances, the failure of the Commissioner to provide any detailed reasoning for this final decision is problematic.

The *Telstra Bundles OMI Report* is somewhat similar to the Medvet report. The most pertinent finding was that Telstra's failure to prevent unauthorised external access to an internal url (which gave access to a database containing personal information) was a disclosure. Again, this finding is covered in a single paragraph providing little detailed discussion of the interpretation of 'disclosure' in the particular circumstances:

---

[1108] *NPP 2 and NPP 4 Email*, above n 1054.

[1109] *Medvet Close Letter 2*, above n 929.

> In general terms an organisation *discloses* personal information when it releases information to others outside the organisation. The Commissioner's investigation concluded that specific errors by Telstra staff led to the Visibility Tool being publicly accessible. The external accessibility of customers' personal information was an unauthorised disclosure and therefore a breach of NPP 2.1.[1110]

The link between a 'release' and unintentional errors leading to the external accessibility of the information is not clearly drawn in either this decision or in Medvet.[1111]

In summary, it is difficult to argue that transparency of decision-making in terms of the development of general principles regarding how privacy laws should be interpreted and the application of those principles in the different cases, particularly in regard to NPP 2, is provided by 5 of the 6 OMI reports considered in this research. In fact, it could be suggested that the OAIC has not given sufficient attention in its decision-making to the importance of developing general principles that can be applied in different fact scenarios. It seems that issues with the way that the different investigations had interpreted and applied NPP 2 and NPP 4 were foreshadowed in an email included in the Dell file. The header and footer of the document have been redacted so that the document context is unclear, although it is described as part of an email dated 24 May 2012.[1112] The document starts with the statement, 'The challenge for us in the future will be to apply the reasoning to different factual scenarios.' It appears to be referring to the OAIC's interpretation and application of NPP 2, and the relationship between 'disclosure', for the purposes of NPP 2, and failing to take reasonable steps for the purposes of NPP 4. It summarises the findings in completed investigations,[1113] noting that:

---

[1110] *Medvet Close Letter 2*, above n 929.

[1111] The proposition that the Medvet and Telstra Bundle decisions support the principle that the failure to take reasonable steps to prevent unauthorised access may be regarded as a disclosure is considered further in the next Chapter.

[1112] *NPP 2 and NPP 4 Email*, above n 1063.

[1113] The document refers to the Sony, Dell/Epsilon, Telstra Bundles and Medvet investigations, together to one other, the details of which have been redacted. Telstra Mail Out and Vodafone are not referred to.

- In relation to Sony, a breach of NPP 2 was not investigated 'because none of their acts or practices were involved in the actual release/access';
- In relation to Medvet, they had caused information to be available on the internet; however, there was insufficient evidence to show the disclosure of personal information, so there was no breach of NPP 2 (although as discussed this outcome was ultimately changed);
- In relation to Dell/Epsilon, there were no acts or practices of the respondents that released the information, so disclosure was not discussed; and
- In relation to Telstra, the posting of an insecure link meant that Telstra 'actually did something' to cause the disclosure.[1114]

This review in May 2012 by the OAIC of the application of NPP 2 and NPP 4 in completed investigations, in the context of considering the future challenge to applying the same reasoning in different factual situations, suggests some awareness that the decisions to that time may not be entirely consistent or reconcilable. Two paragraphs of the email have been redacted on the basis that they go to the OAIC's internal decision-making processes.[1115] It may be that those redacted paragraphs described a coherent framework for the reconciliation of the different decisions that could be applied by the Commissioner in future investigations. If they did, the publication of that framework would be invaluable to those interested in understanding how the Commissioner interprets and applies NPP 2 and NPP 4. This one-page document, out of the over 200 documents produced, is the only internal document disclosed that demonstrates any general consideration of the interpretation or application of NPP 2 or NPP 4 or the two principles working together.

The stated reasons for the OAIC's "new approach" to these investigations (which would have included the publication of the OMI Reports) included the

---

[1114] *NPP 2 and NPP 4 Email*, above n 1054.

[1115] *FOI Act* s 47C.

promotion of public confidence and the provision of transparency of regulatory activities.[1116] It seems likely that these interests, rather than transparency of decision-making, may have been the main reason for the publication of the OMI Reports. If that is this case, it is likely to have also influenced the contents of those reports.

#### 9.10.2.2 Transparency of compliance activities

Public communication about regulatory activity is an important tool for the OAIC, because it may promote community confidence in the OAIC by clearly signalling the way that the OAIC intends to deals with entities that are not complying with privacy laws, and ensuring transparency around the OAIC's use of privacy regulatory powers. [1117] Both of these aims are consistent with the two regulatory frameworks underpinning the Privacy Act.

As discussed, media interest seems to be one of the main reasons for commencing most of the investigations considered in this Part.[1118] The Commissioner engaged extensively with the media over these investigations, confirming that they were being undertaken, and also selecting those investigations to be reported on. [1119] The Privacy Commissioner also believed that media coverage of incidents justified the publication of reports investigation reports. Media interest in the outcome of investigations was specifically referred to as a reason for publishing the OMI report in the Telstra Mail Out case.[1120] The Commissioner also stated an interest in publishing an OMI report on completion of the Medvet investigation 'as it was in the media.'[1121] This heightened level of media engagement regarding these OMIs is consistent with the generally increased media

---

1116 Privacy Commissioner 'Privacy: What's Ahead in 2012?' (Presentation to International Association of Privacy Professionals Australia & New Zealand Annual Summit, 30 November 2011) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-whats-ahead-in-2012>, *OAIC 2012 Annual Report*, above n 1, Chapter 6, 1; *OAIC 2013 Annual Report,* above n 381, 78. See the discussion in Chapter 6.4

1117 *Regulatory Powers Policy, above n 227*, [49] – [50].

1118 See Chapter 9.1.

1119 Ibid.

1120 Email from Helen Lewin, Telstra to Timothy Pilgrim, 26 May 2011.

1121 OAIC, File note, 11 October 2011; referred to in *Medvet Case Management Summary*, above n 920.

engagement noted in Chapter 5.5, both of which may be explained by the OAIC's interest in ensuring transparency of its compliance activities.

However, the Commissioner does not publish reports for all investigations into data breaches that were in the public domain. For example, in February 2012, the Commissioner announced it would be investigating the reported theft of over 10,000 unencrypted credit card details stolen as part of an attack on a system that hosted two Fairfax media sites.[1122] There has been no published report of this investigation. Similarly, when announcing the Sony investigation, the Commissioner referred to a second Sony breach that it would be also be investigating.[1123] No report or statement was made in regard to this second breach. Accordingly, some criteria, in addition to media interest or providing transparency of compliance activities, must be used by the OAIC when deciding which investigations to report.

It could be that OMI reports are published to provide some sort of public reassurance that the Commissioner has resolved major data breach cases. In all of the reports, the Commissioner refers approvingly and in some detail to the remediation efforts of the respondents. For example, the Conclusion section in *Telstra Bundles OMI Report* provides that:

> The Commissioner decided to cease the OAIC's own motion investigation upon reviewing information from Telstra about its remediation project. He found that the remediation steps that Telstra was taking put into place comprehensive data security systems, in compliance with the Act.[1124]

Even in the problematic Medvet investigation it is noted that Medvet 'acted swiftly to identify the security risks to the personal information it holds and has taken

---

[1122] See, eg, Darren Pauli, 'Privacy Commissioner Probes Fairfax Hack', *SC Magazine* (online) 1 February 2012 <http://www.scmagazine.com.au/News/288847,privacy-commissioner-probes-fairfax-hack.aspx >. See also Timothy Pilgrim, 'Privacy Commissioner opens investigation into Telstra hacking incident' (Statement, 22 May 2012) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/telstra-data-breach/privacy-commissioner-opens-investigation-into-telstra-hacking-incident>.

[1123] Timothy Pilgrim, 'Investigation into Sony data breach' (Statement, 4 May 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/sony-playstation-network/investigation-into-sony-data-breach-4-may-2011>.

[1124] *Telstra Bundles OMI Report,* above n 336, 3.

appropriate steps to improve its security systems and develop policies and procedures that reduce identified risks.'[1125]

Findings in regard to the respondents' desire to become compliant are an important consideration when determining the appropriate regulatory response. As has been discussed previously, the Ayres and Braithwaite pyramid supports the use of a more conciliatory approach where the respondent indicates a willingness to become compliant. [1126] The references in these investigations to the respondents' attitude to remediation may be explained on that basis. However, the responsive regulatory approach does not necessarily explain the Commissioner's interest in high-lighting remediation efforts in those cases where no breach is found. For example, the 'Conclusion' section of the *Dell/Epsilon OMI Report* (where no breach was found) refers to the way that Epsilon swiftly identified the cause of the incident and contained the risks to the information it held and took appropriate steps to improve its security systems, which steps 'helped to ensure that the breach was contained and no further unauthorised access occurred.'[1127] The *Sony OMI Report* is similar. Although the OAIC found that Sony had not failed to take reasonable steps to protect the personal information, the OMI report still lists a series of steps taken by Sony under the heading 'Action taken after the cyber-attack.'

An alternative explanation for the OAIC's inclusion of details of the respondents' remediation in each of the OMI reports, including those where there is no finding of breach, may be its interest in reassuring the community that the Commissioner and the respondent have agreed on an appropriate remediation strategy (regardless of whether there was a breach of the Act). This is consistent with the conciliatory approach to resolution of OMIs discussed in Chapter 9.8 above.

A final reason may the Commissioner's belief that it is of benefit to the respondents themselves to be seen to be compliant. In the interview with the researcher, when discussing what outcome the Commissioner looked for from OMIs,

---

[1125] *Medvet OMI report*, above n 338, 2.

[1126] See *Information Sheet 13,* above n 203, and the earlier discussion regarding the compliance approach to enforcement that underpins the Act in Chapter 2.5.

[1127] *Dell/Epsilon OMI Report*, above n 337.

the Commissioner noted that 'in the majority of these cases organisations are obviously going to be willing to [agree to remediation activities] particularly if the matter has been at the forefront of the media.'[1128] He referred to the importance of trust to organisations and how, if organisations have failed to properly secure personal information, they need to 'make sure that they're seen to be taking appropriate steps to remedy it and improve their systems and that's what we're looking for.'[1129] This is the position used by the OAIC to justify publication of the OMI report in the Telstra Mail Out investigation.[1130] It also appears to have been a position accepted by at least one of the respondents. An email exchange in the Vodafone file referred to Vodafone's desire to settle the terms of the report so that it could 'communicate key elements' of the contents of the report 'to allay any remaining customer concerns.'[1131] However, given that reports are not issued for all breach cases that receive media attention, the OAIC's interest in providing respondents with an opportunity to restore trust does not entirely explain the selection of the particular investigations for publication.

#### 9.10.2.3 Deterrence

The third reason given for publishing OMI reports is to act as a deterrent to other entities, by providing some public record of failure.[1132]

There is little indication from the reports themselves that publication was motivated by a desire to deter either the organisation involved or the general community. There is little evidence of language that is critical of any of the respondents. It is difficult to argue that the decision to name the organisation involved or generally to issue more detailed reports about the incidents was intended

---

1128 Interview with Timothy Pilgrim (Sydney, 14 December 2012).

1129 Ibid.

1130 Email from Helen Lewin, Telstra to Timothy Pilgrim, 26 May 2011. A copy of that email is included in Appendix C . A further email repeating these contentions was sent by Helen Lewin, Telstra to Linda King, OAIC, 2 June 2011.

1131 Email from Vodafone to OAIC, 10 February 2011.

1132 See Chapter 7.1.4.

to act as a 'deterrent' given that each of the incidents being investigated were already in the public domain.

In Chapter 7 it was concluded that the stated reasons for the publication of case notes and OMI reports were to provide transparency of decision-making and compliance activities and to perhaps work as a deterrent. Based on the analysis in this chapter, it would seem that the actual reasons for the publication of the 6 OMI reports examined were to provide transparency of regulatory activity and to support community confidence, in the sense of an active regulator appropriately exercising its powers and ensuring that any issues have been addressed. To the extent that transparency of decision-making is intended to be provided, the reports published could not be regarded as meeting that intention.

### 9.10.3 APP Guidelines

Before leaving the issue of the purpose of publishing OMI reports it is worth noting that some of the OMI reports considered in this research have been used to support the Commissioner's interpretations of the new privacy principles in the recently released guidelines to the APPs ('APP Guidelines').[1133]

The OAIC's view that OMI reports have value as precedents or at the very least provide educative examples of the application of principles in different circumstances, which view is not entirely supported by this research, seems to be confirmed by the inclusion of these references in the new guidelines.

For example, the *APP Guidelines* define 'Disclosure' as:

> An APP entity discloses personal information when it makes it accessible to others outside the entity and releases the subsequent handling of the personal information from its effective control. This focuses on the act done by the disclosing party. … The release may be a proactive release, a release in response to a specific request, an accidental release or an unauthorised release by an employee. [1134]

---

[1133] *APP Guidelines*, above n 525.

[1134] Ibid [B.58] – [B.59], 'Chapter B: APP Guidelines Key Concepts'.

Examples are given of what this means, which include 'where an organisation publishes personal information whether intentionally or not[15] and it is accessible to another entity or individual.' The footnote refers to the Medvet and Telstra OMI reports. Given the limited analysis of the definition of 'disclosure' or the basis on which the Commissioner determined there was a disclosure in either case,[1135] the reference to the Medvet and Telstra reports as precedents for the idea of disclosure by publication 'whether intentionally or not' is problematic. In any case, there is no discussion of publishing as disclosure in either of those reports; in fact the term 'publish' is not used at all.

If this interpretation of 'disclosure' had been put to Medvet, the company might have argued that it did not 'publish' the delivery details on the internet; that those details had been cached by Google Analytics without Medvet's knowledge or permission, and that in this case Google was a third party interloper similar to an attacker who accessed the information and made it available publicly without Medvet's authorisation, in response to a search conducted by another unrelated party (in Medvet's case, the 'industry figure'). The discovery of the cached details required significant effort by the industry figure who had alerted the media to the issue. Medvet may still have failed on the reasonable security test and breached NPP 4 because it should have been aware that improper implementation of a web facing application may result in order information being extracted by web tools such as Google analytics. However, Medvet did not have the opportunity to put this case to the OAIC because none of the jurisprudential background for this interpretation or its application in Medvet's circumstances was provided to Medvet. As stated, the term 'publish' was not used at all in the report. Assuming that the second draft OMI report sent to Medvet for its review was the same as the final OMI report (which is reasonable because Medvet made no comment on the draft), accessibility on the internet as disclosure was covered by only two sentences in that report, with no further background or discussion of the meaning of that concept.[1136]

---

[1135] See Chapter 9.10.2.1.

[1136] The relevant section from the OMI report is quoted in Chapter 9.10.2.1.

A similar case could have been put by Telstra, although less convincingly as there was evidence that they knew that the internal url was publicly searchable but they had done nothing to address that. However, this does raise the question as to the point at which the organisation's actions or failure to act amount to 'publication' and thus 'disclosure' for the purposes of NPP 2.

Is any use of the internet by an entity to make personal information available, as commonly happens in every web-based application (for example, those used for event registration, newsletter and update subscriptions and on-line purchasing) a publication and thus a disclosure? If not, where should the line be drawn? Is the test whether access has been limited to authorised users? This would be consistent with the result in *First State Super,*[1137] where an authorised user exceeded his authority and gained unauthorised access to other users' personal information. The OAIC decided that this did not amount to a disclosure by First State Super (FSS) because there was no release of the information outside the organisation. However, it is difficult to differentiate the actions by the FSS member from the industry figure who alerted the press (and ultimately the Commissioner) to the fact that Medvet customer address details could be accessed via a Google search. Does an organisation that makes information accessible via the internet, but which states that it must not be accessed other than by authorised users 'publish' that information if it is accessed by unauthorised users? The reference in the APP Guidelines to 'releasing the subsequent handling of the personal information from its effective control' indicates some further requirement. If the decision depends on the extent to which control over access to the information has been retained, does that become a question of the access controls that were in place? Is the level of access control really a question regarding whether there was adequate security to prevent unauthorised access, as contemplated by NPP 4, rather than a question of 'disclosure'?

Further in the same section in the APP Guidelines, a distinction is drawn between disclosure and 'unauthorised access,' where it is stated that there is no disclosure 'where a third party intentionally exploits the entity's security measures

---

[1137] *First State Super OMI Report*, above n 344

and gains unauthorised access to the information.'[1138] Cyber-attack is referred to as an example of unauthorised access but not disclosure, and the *Sony OMI Report* is again footnoted as a reference for this proposition. Again, given the earlier discussion of the way that the term 'disclosure' is treated in the *Sony OMI Report*, the use of that report as support for the proposition that a disclosure does not include a case of intentional exploitation by a third party is also problematic.

This statement seems to indicate that any unauthorised access by a third party is not disclosure.

This differentiation does not sit easily with the Medvet case where, arguably, the access to the information was not authorised; certainly not in the sense that Medvet knowingly put that information in the public domain or released it outside the organisation or knowingly allowed third parties to access it. It may be that the difference is the intention and action of the third party malicious attacker, which breaks the connection between act of the organisation and the unauthorised availability of the information. The proposition that it was the malicious attacker that influenced the determination of whether there had been a disclosure was put to the Assistant Commissioner Compliance. She confirmed that '[t]he fact of an external access … means that the organisation itself didn't do something to release the information or a failure to take reasonable steps to release that information.' However, this analysis could be equally used for Medvet and Telstra. In both those cases, if the third party had not done its own search, there would have been no unauthorised access.

If the OAIC intends that the term 'disclosure' requires that there be some real causal link between the publisher and the information being publicly available (to distinguish the case of the malicious attacker) then there should be a clearer description of what that link should be. Without this explanation or any other indication of the reasoning underpinning the terminology used in the guidance there is no real transparency regarding the OAIC's interpretation and no guidance in a substantive sense for the regulated community.

---

[1138] *APP Guidelines*, above n 525, [B.60].

## 9.11 CONCLUSION

In summary, the review of the investigations conducted in these 6 cases highlights the following:

- There is no clear use by the OAIC of its own criteria in deciding which incidents should be the subject of an OMI. In particular, none of the 6 investigations reviewed were overtly undertaken on the basis that they involved any systemic issue or that they were a responsive to a perceived risk of significant harm. The main reason for commencing the investigations seems to be the media attention that had been given to the cases, and the Commissioner's own decision to investigate high-profile data breach cases;
- Three of the 6 cases took more than 12 months from the commencement of the investigation to the issuing of the final report. In those cases, the delay related to the time taken to issue the Close Letter or OMI report rather than to the investigation process itself which in most cases was promptly pursued;
- No case plan was prepared to guide any of the investigations. There is no indication from the files of any pre-planning to identify the evidence that should be obtained in each case to determine whether there has been an interference with privacy and no case plan developed for the investigation steps to be taken;
- Rather than specific questioning based on the details of the case, generic and non-specific questions are typically posed in the RFI Letters sent to the respondents, which letters are also the principal device for gathering information about the incidents;
- The investigation process does not seem to involve any vigorous pursuit of information (an example being the OAIC's acceptance of Dell's refusal to provide a copy of its report) although there is a willingness to at least threaten to use more coercive powers in the face of lack of cooperation, as demonstrated by the OAIC's response to Telstra's delay in the Telstra Bundles OMI;

- Communication between the OAIC and the respondents is almost entirely by exchange of emails and letters, with little evidence of any physical meetings or site inspections taking place;
- The evidence relied on by the OAIC in reaching its decisions is provided by the respondents either directly or via third party reports commissioned by the respondents;
- There is no independent testing or verification of the information that is obtained from or at the direction of the organisation being investigated in response to the questions raised in those RFI Letters;
- The OAIC has issues in assessing the evidence that is provided. The office has problems in ensuring it has the skilled resources available to allow it to carry out investigations into complex data breach case. However, the Commissioner believes that the OAIC has sufficient skills to determine the extent to which it should rely on third party reports that are commissioned and paid for by respondent organisations;
- The investigation files provide little information to indicate the process used within the OAIC to arrive at a decision regarding the outcome of an investigation. They do however support an interest by the OAIC in arriving at agreed outcomes from the investigations with the respondents;
- The OMI reports (other than Vodafone) do not provide detailed reasoning, based on findings of fact, to support the decisions made. In the Dell /Epsilon and Sony cases the facts relied on as supporting reasonable steps are of either limited or no relevance to the alleged breach. The findings in the other cases are not clearly linked to the particular facts relied on;
- The decision to publish the reports about these investigations seems to have been influenced by the Commissioner. The decision does not seem to have been made on the basis of the criteria stated in the guidance on publishing case notes;
- The reason for publishing the OMI reports is not clear. The tenor of the published investigation reports seems to reflect concern that the OAIC be able to demonstrate that the incidents had been remediated, either as a

response to media interest or to promote awareness of the OAIC's compliance activity. The reports also seem to reflect conciliated outcomes, rather than administrative decisions.

Applying the conceptual framework developed in Part 1 to these findings:

Generally, the Commissioner's investigations follow a consistent investigatory path that ensures that the main aspects of procedural fairness are addressed. The use of the standard-form RFI Letters and Close Letters helped ensure that the respondents were advised appropriately of the matter being investigated, their rights and the Commissioner's decision. The respondents were also advised of the possible outcomes from the investigation and (in most cases) given an adequate opportunity to respond. Reports from the investigations are published on the OAIC's website, providing some level of transparency.

However, there are a number of other aspects of the Commissioner's use of its investigation powers that may not be regarded as supporting a transparent, balanced and vigorous use of regulatory powers.

The Commissioner's decisions to commence each of the 6 investigations could at best be described as motivated by public interest, rather than by a broader range of goals. Accordingly, it is difficult to characterise the use of the investigation power in these cases as balanced or vigorous.

In terms of the evidence, the use of standard RFI Letters and the absence of individual case plans raise issues regarding the sufficiency of the evidence obtained in each of the different cases. Further issues are raised by the Commissioner's willingness to accept the respondents' evidence without any independent corroboration. Although perhaps an inevitable consequence of the nature of OMIs where there is no complainant or adversary, and no other party to put forward additional facts or an alternative interpretation of the incident, this reliance is not consistent with the suggestion in the *ARC Evidence Guide* that information provided by applicants should be given limited weight.[1139] These issues about the sufficiency

[1139] *ARC Evidence Guide*, above n 238, 3.

of the evidence obtained in regard to the incident go to both the balance and the vigour of the use by the Commissioner of its investigation power.

In terms of the investigation process itself, the Commissioner seems to adopt a perhaps overly conciliatory role in regard to the respondent, eschewing any vigorous independent enquiry into each case or forcing a reluctant respondent to provide information. This approach may be a consequence of the limited powers available as a consequence of an OMI. It may also be a consequence of the limited resources and skills available to the OAIC, particularly when faced with investigating highly complex data security incidents. Whatever the cause, the absence of any testing of the respondent's evidence or detailed questioning regarding the reasons for the breach and the interest in arriving at an agreed outcome all suggest a less than vigorous investigative approach.

The final element of procedural fairness is the extent to which the published reports provide adequate reasons for the decisions made. As discussed, none of the reports, other than Vodafone to a limited extent, could be regarded as meeting the standard for adequacy of decision-making. This in turn means that most of the reports fail to provide real transparency of decision-making, in terms of providing clear evidence of the Commissioner's interpretation and application of the privacy principles.

In summary, although there are some efforts to follow a process that supports procedural fairness, it is difficult to define the Commissioner's use of its investigation powers regarding NPP 4 in the 6 investigations considered as transparent, balanced or vigorous.

Notwithstanding all of the above, an important question for this research remains: Do these 6 investigations support an interpretation of NPP 4 that is consistent with industry practice?

This is considered in the next chapter.

# Chapter 10: Findings - OMIs and Information Security Industry Practice

From the preceding chapter, it is clear that there are issues in terms of the transparency, balance and vigour with which the Commissioner has used its investigation powers in the 6 investigations considered in this Part. However, these issues may not be as critical to answering the questions posed by this research if it can be demonstrated that the OMI reports published as a consequence of those investigations support or, at the very least, could be considered to be consistent with industry practice in regard to ensuring the security of personal information.

As discussed in Chapter 3, the industry approach to information security is comprised of the following:

- Risk: The use of risk assessment as the basis for the identification of risks to assets and the selection of security safeguards to manage those risks;
- Security measures: The selection of administrative controls (including policies and personnel-related controls), physical and technical security controls to manage the risks identified as part of the risk assessment; and
- Process-based approach: The adoption of an iterative process that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks.

This chapter will consider the extent to which the 6 investigations have used an industry practice approach to information security to assess whether the respondents have complied with NPP 4.

## 10.1 INDUSTRY PRACTICE APPROACH TO INFORMATION SECURITY

Although the words 'industry practice' are not used in any of the 6 OMI Reports, there are statements of general principle regarding what is meant by NPP 4 that include all of the elements of the industry practice approach: risk, the selection

of security measures and the ensuing operation of those measures. Such statements are included in 4 of the 6 OMI reports. By comparison, similar statements were included in only 4 of the 23 case notes and 8 OMI reports that considered NPP 4 which were reviewed in Chapter 6.[1140]

The *Vodafone OMI Report* refers to the need for the selection of security measures by the identification of risk and the implementation of policies and procedures to reduce that risk and settings to monitor and measure performance (the three main elements of the industry based security management approach). These are some of the 'range of measures' that should be considered when organisations are 'deciding what security safeguards are reasonable to comply with their obligations under NPP 4.1.'[1141] Almost identical wording is used in the *Medvet OMI Report*[1142] and in the *Telstra Bundles OMI Report*.[1143] Reference to some of the controls listed in ISO 27002 in the *Sony OMI Report* could also be interpreted as reference to the basic elements of an industry approach to information security.

No similar general statement is included in the OMI reports for the Telstra Mail Out or Dell/Epsilon investigations.

It is not clear why the reports diverge in this way. It would be expected that the same statement of general principles regarding how appropriate security measures should be identified and implemented would be referred to in each case. It may be that greater attention to general principles was given in those cases where the respondent was found not to be compliant with NPP 4 (that is, Vodafone, Telstra Bundles and Medvet).

Assuming that the Commissioner would assess reasonable steps by reference to the statements of general principle contained in 4 of the reports, it would be expected

---

1140 See the earlier discussion in Chapters 6.4.2.

1141 *Vodafone OMI Report*, above n 333.

1142 The only difference is the omission of the specific reference to ISO 27002 in the later reports. This is discussed further below in the Section covering references to Standards.

1143 The statement of general principles in the *Telstra Bundles OMI Report* limits the security measures that should be considered to the development of policies and procedures and the training of staff in those policies and procedures, rather than the more general categories of security measures referred to in both Vodafone and Medvet.

that the investigations and reports would focus on the 3 elements identified in those statements: risk assessment, the selection of security measures to remediate identified risks and a process-based system for ensuing the operation of those measures.

The references to each of those elements in the 6 OMIs are considered below.

### 10.1.1 Risk

As noted in Chapter 6, the case notes and OMI reports published prior to 2011 contain few references to risk. [1144] Similarly, there is little consideration of risk in the OMIs under review in this part of the research.

No request for details about the general risk profile of the organisation, the risk assessment processes used by the organisation or any assessment which may have been undertaken around the risk of occurrence of the type of event under investigation was included in any of the RFI Letters. Nor were any questions asked about known vulnerabilities or threats.

As noted, there are references to risk in the Telstra Bundles RFI Letter.[1145] Question 8 asked for information about the 'risks' associated with the disclosure, and how they were being mitigated. This question was not directed at the assessment Telstra had done as part of taking 'reasonable steps' but at the harm that may eventuate from the incident, and the steps Telstra had taken to address that harm. Questions 12 and 13 were directed at what security measures were in place and whether they were believed to be sufficient. Similar questions were asked in the other RFI Letters, however, only the Telstra Bundles RFI Letter uses the term 'risk', asking whether the security measures 'adequately manage the risk.' Telstra's response to this request has been redacted so it is not clear how Telstra responded to this query.[1146] It is also not clear why the Telstra Bundles RFI Letter refers to risk when the others did not.

---

[1144] See Chapter 6.4.

[1145] *Telstra Bundles RFI Letter*, above n 862.

[1146] Email thread from Telstra to Mark Hummerston, between 14 December 2011 and 3 February 2012.

Following the RFI Letters, there is no evidence of the collection by the OAIC of any information that might be relevant to an independent assessment of possible risks in any of the investigation files. There may have been some reference to risk in the letter seeking further information in the Telstra Bundles investigation, which letter alludes to the OAIC's interest in identifying 'all the relevant vulnerabilities that led to the incident.'[1147] The use of the term vulnerabilities is unusual. It is part of the lexicon of information security risk and has not been used in any of the reports, the RFI Letters or other file records. Again, Telstra's response to this letter has been wholly redacted so it is not clear what information was provided in response.

Despite there being no evidence of the collection of risk-related information either directly from the respondents or from third party sources (other than possibly in the Telstra Bundles investigation), risk is specifically referred to in 3 of the OMI reports: the Vodafone, Sony and Medvet OMI reports. The report on the Telstra Bundles investigation, the only case where risk was raised in the RFI Letter, contains no reference to risk.

The issue of risk is dealt with best in the *Vodafone OMI Report*. That report refers to the reasonableness of the steps being based on the risks in the particular business circumstances. It specifically identifies the following as circumstances that added risk in Vodafone's case, that:

- Vodafone's business model included licensed dealerships; and
- Vodafone's business functions required it to collect identity information from customers to comply with obligations to complete 100 point ID verification checks (which meant it held a large database of personal information).

The report also refers to the use of shared login IDs and the resulting 'reduction in the effectiveness of audit trails' leading to inappropriate franchisee practices (referred to as 'Siebel farming' in the OMI report) as a risk. Information security practitioners would characterise the use of shared login IDs as a vulnerability (being the absence of unique login IDs which are a control) rather than a risk. Leaving that

---

[1147] Letter from Mark Hummerston, Assistant Commissioner Compliance to Telstra, 8 March 2012. A copy of this letter is included in Appendix C.

aside, the identification of relevant risks in the *Vodafone OMI Report*, and the subsequent reference to those risks in determining the adequacy of the security measures which were in place, is appropriate and consistent with both industry practice and the Commissioner's own statement of general principle.

The reference to risk in the *Sony OMI Report* is more problematic. Although the report notes that risk should drive the requirement for controls, the risk identified in the report is the risk 'for individuals where information is collected online in one jurisdiction, used in another and stored in another.'[1148] This is a risk for the individual who decides to sign up and use the PlayStation Network (PSN). It is a consequence of the use of the internet to deliver games and one of the problems of the international model used in online business. Although perhaps relevant to Sony's consideration of risks to its relationships with its gaming clients, it is not a significant relevant risk in the context of considering Sony's obligations to secure the personal information that it holds.

Having referred to the importance of risk for security and identifying a largely irrelevant risk, the *Sony OMI Report* does not refer to a number of possible risks that the Commissioner might have noted. The PSN database held the information of over 77 million individuals representing a treasure trove of information for a malicious attacker. Additionally, Sony knew it was a target for malicious attacks. It was on notice that groups such as Anonymous and Lulzec had launched a campaign called 'Operation Payback' in response to litigation Sony had commenced to prevent the modification of PSN controllers.[1149] It was also well known that the PSN system itself was technically vulnerable. Those vulnerabilities had been reported in an open

---

[1148] *Sony OMI Report*, above n 335.

[1149] Details of previous attacks are referred to in Sony's evidence at the US Congressional Hearings: see, eg, letter from Kazuo Haria, Chairman, Sony Computer America LLC to Fred Upton Chairman, U.S. House of Representatives, Committee on Energy and Commerce, 26 May 2011, U.S. House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade Hearing, 'Sony and Epsilon: Lessons for Data Security Legislation.' See also Peter Bright, 'Sony hacked yet again, plaintext passwords, e-mails, DOB posted' *Arstechnica* (online), 3 June 2011 <http://arstechnica.com/tech-policy/news/2011/06/sony-hacked-yet-again-plaintext-passwords-posted.ars>; Erica Ong, 'Sony Pictures says 37,500 customer records exposed' *CNet* (online) 8 June 2011 <http://news.cnet.com/8301-31021_3-20070063-260/sony-pictures-says-37500-customer-records-exposed/>.

forum monitored by Sony employees several months prior to the attack.[1150] It is not clear why reference is not made to these factors. It may be that the problem for appropriate risk identification in the Sony case was one of timing. The Commissioner's investigation concluded before Sony's own investigation into the breach was completed. At that time, little information about the actual vulnerabilities exploited by the attacker was in the public domain. This is discussed further below.[1151]

The Medvet OMI report refers to Medvet putting personal information, including sensitive health information, 'at risk of being compromised by using software with these security flaws.'[1152] Although this is an appropriate identification of the relevant risk, there is little detailed consideration of the assessment of that risk in terms of likelihood of occurrence and consequence (although the 'nature of Medvet's business' is referred to elsewhere in the report) or the threats that could exploit the vulnerability. In this case, there was no malicious attack. An 'industry figure' alerted the media to the issue.[1153]

There is no reference to risk (in the sense of either risk identification or assessment) in the Telstra Mail Out report or the other two OMI reports.

It is difficult to understand why, after making general statements to the effect that security measures should be selected based on the identification of risks and applying that principle to the facts in the Vodafone investigations, the Commissioner does not do so in the other investigations. It may be that the OAIC does not fully appreciate the role of risk in the industry approach to information security, a proposition which has been considered in the review of the *Guide to Information Security* in Chapter 6.2.1. In the interview with the Assistant Commissioner Compliance there was some discussion around whether different investigations plans

---

1150 'Data security expert: Sony knew it was using obsolete software months in advance', *Consumer Reports News* (online), 4 May 2011 <http://www.consumerreports.org/cro/news/2011/05/data-security-expert-sony-knew-it-was-using-obsolete-software-months-in-advance/index.htm>.

1151 See Chapter 10.1.2.

1152 *Medvet OMI report*, above n 338.

1153 Ibid.

were followed for different types of incidents. As part of that discussion, the Assistant Commissioner Compliance referred to hacking cases, where the office would be 'looking at the NPP4 issues with great particularity, trying to ascertain the extent to which the threat could have been anticipated and mitigated against or not.'[1154] The anticipation and mitigation of threats referred to by the Assistant Commissioner is at the heart of risk management. This general observation by the Assistant Commissioner Compliance regarding the way investigations might proceed is of particular interest given the absence of evidence of any investigation of that sort from the investigation files or from the published reports, other than Vodafone.

The Acting Commissioner Compliance also acknowledged the importance of considering individual circumstances in OMIs, noting the nature of principle-based regulation is to make such decisions 'contextual':

> It's about the size of the organisation, the nature of the information that's being held. So there isn't a magic standard because all of those things are going to differ in each context so we do have to apply those factors in relation to each matter that comes along.[1155]

Similarly, each of the OMI reports states that the Privacy Commissioner will consider an organisation's particular circumstances when assessing whether it has taken 'reasonable steps' as required by NPP 4.1, which will include consideration of 'the organisation's size, structure, activities, how it handles personal information and the type of personal information it holds.'[1156]

However, there is no evidence that any of these contextual matters were actually considered by the Commissioner in any of the OMI reports, other than in Vodafone and perhaps Medvet. In the four other cases, there is no link between the general statement of principle (that is, that context is important) and any relevant findings of fact or any application of the general principle to the facts. There are no questions in any of the RFI Letters directed at identifying the specific circumstances

---

[1154] Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012).

[1155] Interview with Assistant Commissioner Compliance (Syndey, 14 December 2012).

[1156] *Medvet OMI report*, above n 338.

of the organisation. There is no evidence of the collection of contextual information from the entities being investigated or from third parties and no material in any of the investigation files that would indicate that relevant contextual information has been gathered from other sources.

The relevant circumstances that gave rise to risk in the Vodafone case have already been considered. In Medvet, the reference to 'putting individuals' personal information, including sensitive health information, at risk of being compromised' could be regarded as contextual. However, the sensitivity of the information is not referred to again in the report nor is there any reference to other contextual details relevant to the determination of what is reasonable, such as the size of the organisation, the extent of its online presence, its value to consumers or the revenues derived from that business. The Commissioner may well be taking these factors into account; however that is not apparent from the OMI reports themselves and does not seem to be supported by the Commissioner's investigation process.

### 10.1.2 Security measures

The second part of standard information security practice is the selection of security measures to reduce the identified risks of loss or harm.

Given the general statements about the need to assess risk (in 4 of the reports) or to consider what is reasonable in the circumstances in each case (which appears in all 6 reports), it would be expected that each report would identify risks and then link the identified risks or relevant circumstances (e.g. the sensitivity of the information, the way it was being handled and the resources of the organisation) to the findings in regard to the security measures in place or not in place, as the case may be. However, in view of the preceding discussion about the failure of the reports to identify risks or circumstances that may be relevant to assessing what is 'reasonable,' it is not surprising that (other than Vodafone) it is difficult to draw from the reports any clear link between risks or the relevant circumstances and the security measures that were missing (thus resulting in a breach of NPP 4) or which were present (ensuring compliance with NPP 4). In the *Vodafone OMI Report*, relevant risks are identified, as are the relevant security safeguards that were in place (in this case, the use of passwords to access the Siebel system and the maintenance of audit trails within the

system). The report then connects the general principles, the identified risks and the adequacy of the security measures in place, stating that:

> [w]hile Vodafone had a range of security safeguards in place … the use of store logins and the wide availability of full identity information via Siebel caused an inherent data security risk in terms of how personal information was protected by Vodafone. For this reason, in the Privacy Commissioner's view, Vodafone had not taken reasonable steps to protect the personal information it held.[1157]

In the other five cases there is no consideration of risk or relevant circumstances which could be used to support the assessment of whether or not the security measures in place are reasonable. If risk or the relevant circumstances are not used to identify what 'reasonable' security measures, it is important to consider whether any alternative method is used.

Each OMI report includes a statement of general principle similar to the following: 'The OAIC will look at the overall security safeguards in place within an organisation when assessing whether it has taken reasonable steps to comply with NPP 4.1.' The idea that there should be more than a single safeguard is consistent with the OAIC's guidance that refers to a 'range of security measures' which should be considered when determining what are reasonable steps,[1158] and with industry practice. Four of the OMI reports (Vodafone, Sony, Dell/Epsilon and Medvet) include a further general statement describing the security measures that should be in place, including physical, computer and network security measures, communication security and personnel security protocols, which are the same areas referred to in the Commissioner's guidance. Within each of these areas, specific measures are referred to such as access controls, firewalls and awareness training. There are small differences in the way the 4 reports describe the relevant security measures. The Medvet report includes a reference to secure storage and destruction facilities. Dell/Epsilon also refers to secure storage and destruction facilities but does not include the reference to 'communication security.' It is not clear why the wording of the general statement changes between the 4 cases or why neither of the Telstra OMI

---

1157 *Vodafone OMI Report*, above n 333.

1158 See *Information Sheet 6*, above n 534; and the *Guide to the NPP*, above 533, 45.

reports includes a similar statement of principle. In any case, the value of including a statement of general principle (that is, that a range of security controls should be in pace) ultimately depends on how that principle is applied in the particular circumstances.

All of the 5 OMI reports other than Vodafone refer to security measures that the Commissioner found to be in place. There is difficulty, however, in identifying how the Commissioner was able to form a view in the circumstances that those security measures found to be in place represented either the taking of reasonable steps or the failure to do so.

In Medvet, the Commissioner appears to have relied on the findings in the report prepared by Deloitte. These findings include that the incident occurred because Medvet used online ordering software that was flawed. According to the OMI report, the Deloitte report found that Medvet needed to implement additional security measures, such as security policies and the standardisation of information security testing and compliance activities and improve its internet facing security. These findings could have been used by the Commissioner as evidence of the failure to take reasonable steps. However, these particular measures were not referred to in the determinative wording in the report, which provided as follows:

> [i]t was clear from the Deloitte's forensics report that multiple security flaws existed in the software … . Medvet was therefore putting individuals' personal information, including sensitive health information, at risk of being compromised by using software with these security flaws.

On that basis, Medvet was found not to have taken reasonable steps. It is possible for software to be flawed, and for organisations to use that software and for reasonable steps to have been taken. Microsoft releases patches to rectify security flaws in its software on the second Tuesday of every month.[1159] Medvet's failure was more probably based on the suggestion in the Deloitte report that if Medvet had conducted testing prior to 'going live' with the online ordering facility, that testing would have identified the flaws, which may have resulted in those flaws being

[1159] See *Patch Tuesday* <http://en.wikipedia.org/wiki/Patch_Tuesday>.

corrected. Medvet's failure to test the software, rather than the use of flawed software, represented the failure to take reasonable steps. A simple linking sentence back to the issues identified in the Deloitte report would have made this clear.

The *Telstra Mail Out OMI Report* lists a number of security measures that were in place. The report states that 'despite these measures being in place' an employee inadvertently used the wrong data table, which meant that the wrong address information was used in the mail-out. There is no indication of the basis on which the Commissioner was able to determine that these measures were appropriate and that the mistake in this case was not indicative of any failure of the system but was a one-off human error. There is no assessment of the risks involved in the mail out or reference to the security measures that might have been implemented based on that risk assessment.

The problem caused by the use of different statements of general principles is demonstrated by comparing the Telstra Mail Out decision to the result in the second Telstra case. In the Telstra Bundles investigation, the Commissioner found that Telstra had policies and processes in place that, if followed, should have prevented the breach, which was similar to the findings in the first Telstra case. However, rather than characterise the failure as a one-off human error (as was the decision in Telstra Mail Out) the Commissioner decided that, in the absence of evidence of behaviours consistent with those policies and procedures, there was a failure to take reasonable steps. This is a clearer decision than that made in the earlier Telstra case because it expressly states that the existence of policies and procedures will not be taken as evidence of compliance with NPP 4 unless it can be shown that organisations are acting on them. It is also consistent with the statement of general principle in the report, which specifically includes monitoring of compliance as part of the Commissioner's view of what are reasonable steps. However, it introduces an element (evidence of compliance) that was not considered as part of the assessment of reasonable steps in the earlier Telstra case. If a similar statement of general principle with reference to the need for monitoring of compliance had been included in the *Telstra Mail Out OMI Report*, a different conclusion may have been reached in that case.

The *Sony OMI Report* demonstrates even more fundamental problems with the Commissioner's reports, with there being little linkage between general statements of

principle, the actual findings of fact and the reasons given for the decision made.[1160] The OMI report includes the following general statements of principle:

- The Commissioner considers a range of measures an organisation has in place when deciding whether it has taken 'reasonable steps;'
- The Commissioner will 'consider an organisation's particular circumstances when assessing whether it has taken "reasonable steps" as required by NPP 4.1'; and
- As part of the assessment of 'reasonable steps', the Privacy Commissioner will have regard to relevant international standards, including ISO 27002.[1161]

Following those general statements, there is the reference to the risk caused by online collection of personal information that has been discussed already. The report then refers to a range of security measures the Commissioner found in place (based on the evidence provided by Sony) including:

- Physical, network and communication security measures to protect the information collected and stored in connection with the Network Platform;
- Encryption of credit card information; and
- Internal information technology security standards that are based on the international information security standard ISO/IEC 27001.[1162]

These high-level descriptions provide virtually no information regarding the types of physical, network and communication security measures that were in place or the actual security standards implemented. It would be possible to be more descriptive about the types of security measures in place without compromising Sony's security; for example, was the network segmented, were application firewalls in place, and was data transmitted using some sort of secure tunnelling protocol such as SSL?

---

[1160] See Bloom and Frketic, above n 1100, 5, who compares the written reasons provided by the ICO as part of its investigations to those of the OAIC.

[1161] *Sony OMI Report*, above 535, 1.

[1162] *Sony OMI Report*, above 535, 2.

The *Sony OMI Report* continues:

> Despite these measures, the security of the Network Platform was compromised as a result of a targeted cyber-attack. … A targeted attack on an organisation does not necessarily mean that the organisation has failed to take 'reasonable steps' as required by NPP 4.1. Based on the information provided by SCE Australia to the Privacy Commissioner, including information about the range of security measures in place at the time of the incident, the Privacy Commissioner found that reasonable steps had been taken … [1163]

There is no direct link between 'the range of security measures in place at the time of the incident' and the earlier list. Even if there had been, it would have provided very little further detail in terms of the security measures which the Commissioner determined were reasonable in the circumstances (given the high level and non-exhaustive list provided), or the basis on which the Commissioner was able to come to that decision. There is no evidence that the 'appropriateness' or otherwise of the high-level measures referred to in the report was assessed by the Commissioner by reference to any real consideration of risk or the particular circumstances.

The report's failure to describe why the particular controls referred to were regarded as reasonable may be because the Commissioner did not have sufficient detail about how the incident occurred at the time of the investigation. Unlike the Dell/Epsilon report, which contains a quite detailed analysis of the way an employee's device was exploited to gain access, there is no description in the *Sony OMI Report* of how the attack took place. At the time the Commissioner finalised its investigation (effectively in May 2011), Sony had not concluded its own investigation into the incident. This is clear from a written statement that Sony submitted at about the same time to a US Congressional Hearing to the effect that the incident was still being investigated and the cause of the incident was not clear.[1164] It

---

[1163] *Sony OMI Report*, above 535, 2.

[1164] See, eg, letter from Kazuo Haria, Chairman, Sony Computer America LLC to Fred Upton Chairman, U.S. House of Representatives, Committee on Energy and Commerce, dated 26 May 2011 referred to in n 1149.

seems unlikely that Sony would have provided different information to the Australian regulator. Without knowing how the attack succeeded (in particular, what vulnerabilities were exploited so as to allow the attackers access to the information and the ability to extract it) it is not clear how a determination regarding whether or not reasonable steps were in place could be made by the Commissioner.

The UK ICO's report into the same incident was not issued until early 2013, over 12 months after the finalisation of the Commissioner's investigation.[1165] That report benefited from detailed information from Sony about the vulnerabilities in the Sony systems that enabled the attack. By reference to those vulnerabilities, and the failure to implement fairly rudimentary measures such as software patching, the UK ICO decided that Sony had failed to take reasonable steps.[1166] Sony's out of date software patching (which was one of the contributors to the success of the attack according to the UK ICO's report) was not referred to as a relevant consideration by the Commissioner.

Following publication of the UK ICO's report, the Commissioner released a statement which confirmed that '[t]here are no plans to re-open the OAIC's investigation into this matter', the Commissioner being satisfied, 'as is the ICO', that Sony has made appropriate changes to its systems following the incident in terms of the extra security measures that have been implemented to help protect personal information.[1167] This statement is consistent with a view that a significant purpose of publishing OMI reports is to provide community confidence that issues have been addressed, which has been discussed in the previous chapter.

---

1165 UK Information Commissioner's Office, "Data Protection Act 1988 Monetary Penalty Notice Dated: 14 January 2013 Name: Sony Computer Entertainment Europe Limited"<http://ico.org.uk/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx>.

1166 See Tsacalos and Verzi, above n 67. The authors query whether the ICO and the OAIC 'came to different conclusions with the same understanding of the facts, or whether the Australian regulator's understanding was less complete than that of its UK counterpart.'

1167 Office of the Australian Information Commissioner, 'Sony PlayStation Network – Statement from Australian Privacy Commissioner, Timothy Pilgrim' (Statement, 25 January 2013) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/sony-playstation-network/sony-playstation-network>.

Finally, it is worth mentioning that, as noted in the previous chapter, the *Sony OMI Report* lists a series of steps taken by Sony to improve its security following the attack. It is not clear why the failure to take these steps before the attack was not considered relevant to the decision whether or not Sony had taken reasonable steps.[1168]

As discussed, the *Dell/Epsilon OMI Report* is somewhat different to Sony in that more detailed information was available about the breach at the time of the Commissioner's investigation, Epsilon having completed its own investigation. However, the report demonstrates the same failure to connect the security measures in place with risk or to provide detailed reasoning regarding how the Commissioner was able to form the opinion that both Dell and Epsilon had taken reasonable steps in the circumstances.

The report is particularly lacking in detail about Dell's obligations to take reasonable steps to ensure that its contractual partner, Epsilon, secured the personal information it received from Dell about Dell's customers. This was exactly the type of case that the Commissioner had identified as of risk in the Sony report (where the information of Australians is sent out of the jurisdiction). The Commissioner had an opportunity to make a very clear statement about its expectations in regard to Australian-based organisations that send personal information to entities outside of the jurisdiction, but failed to do so. Instead, the report focuses on Epsilon, stating that 'the incident could not have been avoided by any action taken by Dell Australia.'[1169]

This is not necessarily true, as the steps taken by Epsilon were part of the contractual arrangements between Dell and Epsilon. So, to the extent that Dell negotiated those terms, it did have some effect on the security that was in place, which in turn was relevant to the success or otherwise of the attack. A schedule containing the security provisions in the contract between Dell and Epsilon was

---

[1168] See Chapter 9.10.2.2.

[1169] *Del/Epsilon OMI report*, above n 537.

provided to the Commissioner.[1170] This meant that the Commissioner had the opportunity to consider the adequacy of those provisions and provide some general guidance regarding how it was able to determine that they were appropriate. However, no detailed comments are made in the report in regard to those contractual terms. The report contains one paragraph in relation to the contract between Dell and Epsilon, which makes no reference to the actual contractual terms:

> In the Commissioner's view, by entering into the contractual agreement with Epsilon, Dell Australia had reasonable steps in place to protect the personal information it holds from misuse and loss and had met its obligations under NPP 4.1.[1171]

Having absolved Dell of any responsibility because it had a contract in place with a reputable organisation, the report goes on to consider whether Epsilon had taken reasonable steps. Reference is made to the security measures that were in place, such as an ISO 27001 and ISO 27002-compliant information security system. The report also refers to the attack as the consequence of an employee inadvertently allowing malware to be installed on Epsilon's system, which subsequently allowed an attacker to gain access to personal information stored on Epsilon's database. Notwithstanding that this was a very different sort of attack, the findings section is virtually identical to the Sony findings, noting that this was a 'sophisticated and malicious attack,' the occurrence of which does not necessarily mean that the organisation has failed to take 'reasonable steps' as required by NPP 4. On the basis of information received from Epsilon, the Commissioner considered that at the time of the incident Epsilon had reasonable steps in place.

As in the Sony case, there is no reference to risk, there is no direct link between the incident and the specific controls which the Commissioner regarded as pertinent (although presumably they are those listed earlier in the report) and the basis on which those controls are determined to be 'reasonable' is not made clear. The

---

[1170] Dell incident report with attachment: a cop of the Dell subscriber notification email plus Schedule B – Information Security Schedule Dell/Epsilon attached to Letter from Caren Whip to Jodie Siganto, 30 August 2013; schedule item: Schedule A_Dell 6. This document was redacted in its entirety.

[1171] *Dell/Epsilon OMI Report*, above n 537, 2.

reference to the attack as 'sophisticated and malicious' and requiring 'expert knowledge to execute' seems to obviate any need to look more closely at what the organisation might have been able to do to thwart the attack.

As in the Sony report, reference is made to actions taken by Epsilon to 'remediate' the damage caused by the breach. These actions included steps to block and prevent access to bad IP addresses, improvements to virus and malware scanning, changes to procedures for setting and using passwords, and changes to user access to Epsilon's email marketing platform application. Media reports indicate that Epsilon also implemented a number of other post-incident security enhancements including two-factor authentication.[1172] As in Sony, there is no consideration in the report of whether these security measures should have been in place at the time of the attack.

In summary, other than in the Vodafone report, it is difficult to determine the basis on which the Commissioner has been able to determine the adequacy or otherwise of the security measures in place in the cases under review. In most cases, the material findings either do not specifically refer back to the more general findings of facts, or are so general as to provide no guidance regarding what was relied on.

### 10.1.3 Process-based approach

The third element of the standard approach to information security is an iterative process-based approach to security management. This approach is recognised as part of reasonable security in those 4 reports that include some statement representing general practice.[1173] However, this element is not specifically considered in any of the reports, other than Telstra Bundles.

The information security management system based on ISO 27001 that was implemented at Sony and the ISO 27001 compliant system in place at Epsilon may well have supported the sort of governance and iterative continual improvement process that forms part of an industry practice approach. However, the reports do not

---

[1172] Mike Lennon, 'Epsilon Bolsters Security: Shares Details Following Massive Data Breach' *SecurityWeek* (online), 29 June 2011 <ttp://www.securityweek.com/epsilon-bolsters-security-shares-details-following-massive-data-breach>.

[1173] These are the Vodafone, Sony, Telstra Bundles and Medvet OMI reports.

specifically refer to the presence of that continuous process as a relevant and necessary element of 'reasonable steps'.

In the *Telstra Bundles OMI Report*, it is lack of evidence of monitoring of compliance with policies that was determined to be the failure to take reasonable steps in that case. As discussed in the previous section, this finding is in contrast to the earlier Telstra decision where the existence of policies and procedures seemed to be sufficient (without evidence of their operation).

The failure to recognise that information security management is an ongoing process that must be continually monitored and adjusted based on the effectiveness of the controls and the changing risk profile of the organisation, is consistent with the proposition that the OAIC may see information security as a single point problem, resolved by a single solution. For the reasons discussed in Chapter 3, information security is more complex than this. If this is the Commissioner's view of information security, it is out of step with industry practice and inconsistent with the most widely used industry standards: ISO 27001 and ISO 27002.

## 10.2 REFERENCE TO STANDARDS

Three of the OMI reports contain references to the ISO security standards: ISO 27001 and ISO 27002.

The OAIC had obtained a copy of ISO 27002 as part of the Vodafone investigation. A file note (from the Sony investigation file) records that that standard was to be used to 'assess Vodafone's NPP 4 compliance.'[1174] However, there is no evidence of any reference to or other use of that standard in the Vodafone investigation. There is no indication from the investigation file of the use of ISO 27002 in reaching the decision regarding whether or not reasonable steps had been taken (although it should be noted again that any material that related to the OAIC's decision-making processes was redacted from these records). Notwithstanding this, ISO 27002 is referred to in the Vodafone OMI report as part of the statement of general principle about the range of measures that should be considered in deciding

[1174] Internal email thread from LK to AM, 6 May 2011.

what security safeguards are appropriate. (This statement has been considered in the previous section). The report describes ISO 27002 as containing advice about 'information security management protocols that organisations should take into account when designing systems including user access controls and system monitoring.'[1175] Although not inaccurate, this description does not clearly articulate the risk-based system of processes incorporating a range of security measures from different domains that is described in ISO 27002, together with the companion standard ISO 27001.

Only one of the RFI Letters refers to standards, the letter sent to Dell. This letter asked that Dell provide information in regard to the steps Dell had in place to protect personal information, including 'reference [to] any relevant industry standards.'[1176] This is consistent with a note on the Complaint Assessment Sheet: 'Ask what reasonable steps R takes to comply with its NPP 4 obligations. Refer to any relevant industry standards.'[1177] No questions were raised in any of the other RFI Letters in regard to the use of standards generally or ISO 27001 or ISO 27002 in particular, including those investigations where reference is made to these standards in the final reports.

It is not clear where this interest in standards came from. Dell's data breach notification letter does not refer to standards. It may have come from background information given in the initial phone contact in which Dell notified the OAIC of the data breach. It may be that attachments to the data breach notification letter raised compliance with standards.[1178] It is likely that Schedule B - Information Security Schedule, which covered the security measures Epsilon was contractually obliged to maintain, included reference to standards, probably ISO 27001, particularly given the later statements by Dell that it reviewed Epsilon's compliance with relevance

---

1175 *Vodafone OMI Report*, above n 333.

1176 Letter from Mark Hummerston, OAIC to Dell, 16 April 2011.

1177 OAIC, File note, 6 April 2011.

1178 According to the letter from Caren Whip to Jodie Siganto, 30 August 2013, a copy of Dell's Incident Report and of Schedule B – Information Security Schedule, the schedule to Dell and Epsilon contract, were included as attachments to the notification letter.

standards. [1179] Unfortunately, all attachments were exempted in full so it is not apparent the extent, if any, to which standards were referred to in either of those documents.

The premise that the interest in standards was not initiated by the Commissioner but was a reaction to information provided by Dell is supported by a file note that suggests a failure within the OAIC to appreciate the difference between the two main standards, ISO 27001 and ISO27002. The note made by the Compliance Officer on 1 July 2011 (the first activity on the file after receipt of the 10 May response from Dell) states: 'File discussed with supervisor (LK). Issues for follow up standards and investigation report… LK to contact Standards Australia to clarify the content of ISO 270001 (as we have AS/NZS 27002 only under licence).'[1180]

There is no record in the investigation file of whether that contact took place, what clarification was sought or the outcome of any other discussion around standards.

The OMI report states that '…Epsilon applied recognised industry standards including: …for the past five years it has implemented and maintained an information-security program conforming to data security standards set forth by … ISO 27001 and ISO 27002.'

It is likely that this finding is based on information provided by Epsilon, rather than on the OAIC's own independent investigation. The investigation records provided to date give no indication regarding what information Epsilon provided to the OAIC to enable it to make this finding. However, Epsilon has provided information about its ISO 27001 compliant system that implemented ISO 27002 controls in a statement submitted to a US House Committee:

> To enhance security across its infrastructure, Epsilon for the past several years has implemented and maintains an information security program conforming to data

---

1179 Ibid.

1180 OAIC, Complaint Management System Report Epsilon Investigation File. A copy is included in Appendix C.

> security standards set forth by [ISO]. More specifically, Epsilon has implemented an ISO 27001 compliant information security management system that implements ISO 27002 controls. … Epsilon has been ISO 27001 certified since 2006 … [and] has maintained its ISO 27001 certification every year since then.[1181]

It might be assumed that this same information was provided to the Commissioner in response to the RFI Letter. However, there is no indication from the OAIC files that Epsilon was asked to provide any further detail about the information security management system it had in place. Pertinent questions that a person knowledgeable with ISO 27001 may have asked might have included: what was the scope of the certified management system (did it include the server, data base, network and remote devices that were compromised as part of the attack); did the risk assessment completed as part of the ISO 27001 certified system identify the possibility of the attack that had occurred; what specific security measures were in place to address that risk; when had those measures last been checked; when was the system last audited by a third party and were there any relevant outstanding items from that audit?

The Sony investigation progressed at roughly the same time as the Dell/Epsilon investigation, certainly in the opening stages. In contrast to the Dell/Epsilon investigation, no information was sought about compliance with standards in the Sony RFI Letter.

The absence of any questions about compliance with standards in the Sony RFI Letter was raised in the email thread posted by Dr Clarke discussed in the previous Chapter.[1182] Dr Clarke noted the non-specificity of the questions that the Commissioner said had been put to Sony, referring in particular to questions around risk and standards. He suggested that the questions posed to Sony could have included 'how do the security measures that were in place line up against industry standards?'[1183]

---

[1181] *Fitzgerald Statement*, above n 891.

[1182] *Roger Clarke email*, above n 981. See Chapter 9.6.

[1183] Roger Clarke, above n 989.

The proposition that the use of industry standards in particular was discussed internally within the OAIC as a consequence of Mr Clarke's comments is confirmed by the following email which was part of the same email exchange:

> We have got a licensed copy of the ISO IT Security Standard to assess Vodafone NPP4[.] I expect that standard is going to come in handy again and can relevantly be applied to the Sony issues because it is an international standard.[1184]

It is likely that this is a reference to ISO 27002, as that was the standard referred to in the *Vodafone OMI Report*.[1185] The wording of the comment suggests that at least at that time the OAIC regarded ISO 27002 as the only ISO IT Security Standard. There is no reference to ISO 27001 or to the fact that ISO 27002 is designed as a code of practice supporting ISO 27001. The proposition that at the time the OAIC compliance team was not aware of ISO 27001 or its relationship to ISO 27002 is supported by the subsequent note in the Epsilon file already mentioned, which refers to contacting Standards Australia to 'clarify the content of ISO 27001.'[1186]

It is hard to determine why the *Sony OMI Report* uniquely includes a paragraph stating that '[a]s part of the assessment of "reasonable steps" the Privacy Commissioner will have regard to relevant international standards,' referring then to sections of ISO 27002. It may be that the OAIC needed to demonstrate publicly (in response to Mr Clarke's published comments) that industry standards had been considered and so included reference to ISO 27002 in the *Sony OMI Report*. It is also not clear why ISO 27002 was singled out for reference as the relevant international standard. As mentioned, at the time the Close Letter was being drafted and perhaps even at the time of the preparation of the *Sony OMI Report*, which was finalised in mid-September 2011, it is possible that the OAIC had not clarified the difference between ISO 27001 and ISO 2002. There is certainly no reference in the

---

1184 Internal email, OAIC, 6 May 2011.

1185 *Vodafone OMI Report*, above n 333.

1186 CMS Report Epsilon Investigation File, Epsilon Redacted Documents Document 1. A copy is included in Appendix C.

Sony, Dell or Epsilon investigation files to the OAIC obtaining a copy of ISO 27001 or meeting with Standards Australia.

Having specifically referred to ISO 27002 as part of the general understanding of what was required by NPP 4, the final *Sony OMI Report* refers to compliance with ISO 27001 (a different standard) as part of the 'range of security measures' that the Commissioner found that Epsilon had in place in order to meet the obligation to be reasonable. Again, as in the Dell/Epsilon case, it is not clear where the information regarding Sony's compliance with ISO 27001 came from (as those records have been redacted); however, it is again consistent with information provided by Sony to a US Congressional Hearing.[1187] It may be that the OAIC repeated the information provided by Sony without any detailed understanding of what that might mean This would be consistent with the nature of the 'on the papers' investigation that was conducted, where reliance is placed on the information provided by the respondent with little or no independent investigation. . In any case, the result is that the OMI report refers to Sony as being ISO 27001 compliant without reconciling that finding of fact to the earlier general statements about the ISO 27002 security measures that should be considered.

There is a single reference to standards in the Medvet OMI report: 'Monitoring and measuring performance against Australian and International Standards' is included in the range of security measures that may be taken. There is no other reference to the adoption of, or compliance with, any standard by Medvet, or the implications of that in terms of determining whether reasonable steps had been taken.

There is no reference to the use of standards at all in either the Telstra Mail Out or the Telstra Bundles investigations.

In summary, it could be suggested that the Commissioner did not have a detailed understanding of the risk-based management approach to information security that ISO 27001 and ISO 27002 describe or of how that approach should be

---

[1187] U.S. House Energy and Commerce Subcommittee on Commerce, see above n 839.

referenced when considering whether an organisation has taken 'reasonable steps' for the purposes of NPP 4, at least at the time that these 6 investigations were undertaken. There is certainly no evidence of a consistent approach to standards in these cases, whether as part of a general position as to what are reasonable steps or as one of the range of security measures that might be selected or as evidence of the implementation of reasonable steps in the particular case.

## 10.3 USE OF GUIDANCE

Guidance issued by the Commissioner in regard to its interpretation of NPP 4 has been considered in Chapter 6.2.

There is no explicit reference to the specific guidance in relation to NPP 4 provided in *Information Sheet 6* in any of the cases under review. There are two references to the *Data Breach Notification Guide* — both in relation to a discussion of the breach notices sent out by Telstra in the Telstra Bundles investigation[1188] and Sony.[1189] There are however, a number of references to the more general guidance document published in 2001 following the passage of the new NPPs, the *Guidelines to the National Privacy Principles*.[1190] These guidelines are referred to as the source of the definition of the term 'discloses' for the purposes of the application of NPP 2 in the Sony, [1191] Telstra Bundles[1192] and Medvet OMI reports. [1193] It is not clear why only 3 of the reports reference these guidelines when 5 of the reports include a statement in approximately similar terms.

---

[1188] See *Telstra Mail Out OMI Report*, above n 334, footnote 4.

[1189] Under the heading 'Conclusion' in the *Sony OMI Report*, above n 335: '… given his concerns over the period that elapsed before Sony notified its customers, the Privacy Commissioner strongly recommended that Sony review how it applies the OAIC's Guide to handling personal information security breaches.'

[1190] *Guidelines to the NPPs*, above n 533.

[1191] See *Sony OMI Report*, above n 335, footnote 3.

[1192] See *Telstra Bundles OMI Report*, above n 336, footnote 2.

[1193] See *Medvet OMI report*, above n 338, footnote 1.

In relation to the interpretation of NPP 4, the *Telstra Bundles OMI Report* includes a footnoted reference to the *Guidelines to the National Privacy Principles* as the source for the statement that:

> Whether measures taken to secure personal information are considered to have been 'reasonable steps' will depend on the organisation's particular circumstances. For example, the size of the organisation, how the organisation handles the personal information it holds, and the type of information that it holds will be relevant factors.[1194]

It is not clear why these general *Guidelines* were chosen for reference over the more specific guidance in *Information Sheet 6*. This same statement is included in all 6 OMI reports under review, as is the statement that an organisation will need to have a range of security safeguards in place to protect the personal information it holds, which is included in the *Tips for Compliance* section of the *Guidelines to the National Privacy Principles*.[1195] It is not clear why these statements that were included in the other OMI reports do not also refer back to the guidelines.

## 10.4 CONCLUSION

This chapter has considered the extent to which the findings in each of the 6 case study investigations could be regarded as based on an industry practice approach to information security, which should in turn be ascertained by reference to 3 interlinking steps:

- The use of risk assessment as the basis for the identification of risks to information assets and the selection of security safeguards to manage those risks;
- The selection of administrative controls (including policies and personnel-related controls) and physical and technical security controls to manage the risks identified as part of the risk assessment; and

---

[1194] See *Telstra Bundles OMI Report*, above n 336, footnote 2.

[1195] *Guide to the NPPs*, above n 536 , 45.

- The adoption of an iterative process that incorporates the risk assessment outcomes and regular monitoring and testing to ensure that the security safeguards remain appropriate for the management of the identified risks.

The relevant investigation files and OMI reports suggest that the OAIC may have little understanding of what is meant by either a risk-based information security management system or the idea of risk itself. Risk is referred to in a way that is confusing (for example, in the Telstra Bundles RFI Letter where it is conflated with harm) or irrelevant (for example, the risk of dealing with online businesses referred to in Sony). None of the reports (other than Vodafone) indicate that consideration was given to any relevant risk factors, just as the investigation files do not show the collection of any relevant information to support that consideration. Nor is there any evidence that the adequacy of security measures that were in place was assessed by reference to risk or any other measure. This is notwithstanding the reference to the use of risk as the basis for the selection of security controls in the statements of general principle as to what is required by NPP 4 included in 4 of the 6 OMI reports.

The same comment applies to the consideration of relevant contextual issues in the determining of reasonable steps. Although a general statement is made in all of the OMI reports that what is reasonable will depend on the organisation's particular circumstances, there is little evidence of consideration being given to circumstantial matters such as the size of the organisation, the type of information held and how that information is handled (other than in the Vodafone investigation).

The findings in regard to the security measures that were in place in all of the reports other than Vodafone are so high-level as to be of no real assistance in determining what might be reasonable. In any case, it is arguable whether the security measures referred to in the reports were of real relevance to the incidents being investigated, certainly in the cases of Sony and Dell/Epsilon. The reports also generally fail to link the general findings of fact to the material findings that underpin the decision regarding whether there had been a breach of NPP 4.

The OMI reports show little concern about the existence of the iterative continuous improvement process that should underpin an information security management system. There is no evidence of any inquiry into the existence of this process approach, other than identification of the need to monitor compliance in the

Telstra Bundles report. In summary, other than Vodafone, the OMI investigations do not support an industry practice approach to information security.

The references to ISO 27001 and ISO 27002 in the OMI reports suggest that the OAIC does not have a good understanding of the systems and practices contained in those standards. This is consistent with findings in the previous chapter in regard to the skills and resourcing challenges faced by the OAIC, particularly in regard to complex data breach cases.

To the extent that the Commissioner has issued guidance regarding its interpretation of NPP 4, there is little evidence that this guidance has been followed or applied in the investigations. There are few references to the OAIC's own guidance in any of the decisions and none to detailed guidance such as *Information Sheet 6*.

Contrary to the their intended purpose, the reports do not explain the Commissioner's interpretation of NPP 4 nor do they, in substance, illustrate the application of NPP 4 in particular fact circumstances. In fact, the OMI reports provide little indication of the use of any benchmark, reference point or principles to inform the decision regarding whether there has been a breach of NPP 4. These findings are consistent with the assessment of the adequacy of reasoning and transparency of decision-making contained in the general analysis of the reports in the previous chapter. The absence of both adequate reasons and transparency of decision-making raises questions regarding the purpose of these OMI reports. If they do not assist in the interpretation and application of NPP 4 by the organisations who must comply with them, then at best they must be considered a mere record of the Commissioner's compliance activities. Moreover, the failure of these investigation reports to provide valuable guidance or education raises questions regarding the regulator's ability to provide the guidance and education in relation to compliance with NPP 4 that is fundamental to the successful operation of a principles-based regulatory system.

# Chapter 11: Conclusions

The occurrence of data breaches that compromise the security of personal information held by Australian corporate entities is an issue of growing concern. NPP 4 and its successor APP 11 are the only generally applicable legislative provisions in Australia that require organisations to secure personal information. Accordingly, the operation of this provision is important to the protection of the personal information of Australians.

The question considered by this research is: *To what extent is the exercise of the Commissioner's investigation and oversight powers in relation to NPP 4 an appropriate regulatory response?* The answer to this question was broken into three sub-questions:

1. What oversight and investigation powers are available to the Privacy Commissioner?
2. What is the relationship, if any, between the exercise of those powers and recognised industry practice in Australia?
3. To what extent is the exercise of those powers consistent with principles for the exercise of regulatory powers?

The Commissioner's oversight and investigation powers were identified in Chapter 2. It was noted that these powers were consistent with the regulatory frameworks that underpin the *Privacy Act*. Expectations regarding the use of these powers that were derived from those regulatory frameworks were also referred to. In particular, the issuance of guidance and education regarding the Commissioner's interpretation of the privacy principles and the Commissioner's use of a responsive regulatory approach to ensuring compliance were recognised as key to solving the interpretative risks inherent in principle-based regulation, and to ensuring that appropriate outcomes were achieved. A two-part framework for considering the exercise of the Commissioner's powers was developed. It first used principles of transparency, balance and vigour to assess the Commissioner's use of its oversight and investigation powers in answer to the third sub-question. This component was

developed in Chapter 2. A second component, an industry practice approach to information security, was developed and described in Chapter 3 and used to answer the second sub-research question.

The Commissioner's use of its oversight functions, including the provision of guidance, monitoring and auditing, advice and education, was considered in the context of NPP 4 in Chapters 5 and 6. A number of findings made in Chapters 5 and 6 are worth repeating.

There is little evidence of any proactive use by the Commissioner of its oversight powers in regard to NPP 4. In particular, there is no indication that the Commissioner monitors compliance with either NPP 4 or the Act more generally. It is difficult to regard the Commissioner's use of the audit power as either proactive or fulfilling any general monitoring requirement. The total number of audits conducted is low and limited to ACT agencies and a handful of federal agency systems. Accordingly, the audits done to date could not be regarded as offering any more general view of compliance across federal government agencies. There is no clear benchmark used in any of the reports for assessing whether the security measures in place are sufficient for the purposes of IPP 4 and no references to the elements of the industry practice approach to information security used in this research. However, the publication of audit reports does provide some transparency as to the Commissioner's audit process.

Although there has been some increase in the education and advice work undertaken by the OAIC generally, particularly in terms of explaining the recent changes to the *Privacy Act*, there is little evidence of the use of those powers to clarify the OAIC's interpretation of NPP 4 (other than general exhortations to business to be aware of their security obligations and support of data breach notification). The OAIC encourages the reporting of data breaches and refers to its dealing with reported data breaches as part of its advisory functions. However, it is not clear how these activities assist in a more generally educative way.

Prior to April 2013, the OAIC's guidance in regard to NPP 4 was high-level, referring generally to the types of controls that should be in place, and was also somewhat out of date. The new *Guide to Information Security*, although more current, remains high-level and incomplete. It deals poorly with risk assessment (a

fundamental element of the industry practice approach to information security) and does not provide any overarching framework for the selection and management of security controls. It cannot be regarded as entirely consistent with the industry approach to information security put forward in this research. Given the 12-year gap between this guide and the issuance of the previous guidance specific to NPP 4, it also is hard to argue that the Commissioner's guidance power has been exercised in a vigorous way regarding NPP 4.

Consideration of the Commissioner's use of its guidance functions also included a review of case notes and OMI reports published prior to February 2011, which concluded that:

- There is only limited reference to general principles that could be equated to any of the elements of an industry practice approach to information security. There were also only isolated instances where the particular circumstances of the case and the impact of those circumstances on determining what were reasonable steps was considered;
- There were few references to the Commissioner's own guidance, industry standards such as ISO 27001 and 27002 or other decisions made;
- The reports generally provided only limited transparency in terms of clearly stating the reasons for the decisions based on the relevant findings of facts in the particular circumstances; and
- Both the case notes and OMI reports showed an interest in closing the case without necessarily making any finding regarding whether the respondent had complied with NPP 4. This was particularly evident in the OMI reports where post incident rectification steps were taken into account in determining whether there had been a breach of NPP 4.

Generally, findings from the review of the case notes and OMI reports are consistent with the earlier view that the Commissioner's use of its oversight powers does not support an industry practice approach to information security and could not be regarded as transparent, balanced and vigorous.

Part 3 of this research involved a detailed consideration of the Commissioner's use of its investigation powers, by reference to 6 own motion investigations. The

findings made in Chapters 9 and 10 support the findings from Part 2 and also revealed further issues. First, in regard to the investigation process itself:

- In each of the 6 OMIs considered, the decision to commence an OMI appeared to be based on the same single criteria: the need to respond to the media coverage of the incident. There was no evidence, for example, of consideration of whether there was a systemic issue to be addressed or the harm that may have been caused by the incident;
- From the investigation files, the process by which these particular investigations were selected as the subject of OMI reports is not clear. However, it does seem that in most cases the Commissioner was directly involved in both the selection of the case for public reporting and in the finalisation of the published reports;
- There is no indication of the preparation of any case plan or other consideration of issues raised by the particular facts of any of the different cases that may have been relevant to consideration of the evidence needed to determine whether there had been an interference with privacy;
- The Request for Information Letters issued as the basis for the collection of information in each investigation were largely generic and non-specific and could not be regarded as, in themselves, sufficient to ensure all relevant evidence was collected;
- The OAIC used an 'on the papers' investigatory approach which means the investigations were almost entirely based on the information provided by the respondents or consultants retained by those respondents in response to the RFI Letters without any independent testing of the veracity or completeness of that evidence or assessment of whether additional information should have been obtained;
- In the published OMI reports, the links between the findings of facts and the reasons for reaching a particular decision are either unclear or not made at all. The only exception to this is the Vodafone decision. However, even in the Vodafone case, there is no indication of the standard used by the OAIC in arriving at its decision in regard to whether 'reasonable steps' had been taken for the purposes of NPP 4; and

- The references in each of the reports to the remediation efforts made to address any issues and to the cooperation by the respondent during the investigation suggest that the investigations were conducted with a view to being able to state that the incident had been adequately dealt with by referring to the remediation actions taken or being taken.

In terms of the OAIC's reference to industry practice or relevant standards or use of its own guidance in coming to decisions, the 6 OMI cases reviewed support the following:

- The files and the OMI reports indicate that there is no real understanding of risk as part of the information security management process within the OAIC. There is no identification of relevant risks in terms of threats or vulnerabilities and no attempt to link the selection and implementation of security measures to mitigation of identifiable risks, having regard to the level of risk based on an assessment in terms of likelihood and consequence of the risk occurring;
- There are few references to the need for an iterative, continuous improvement process-based approach to managing information security. The Telstra Bundles case recognises the need for ensuring that processes are followed but falls short of placing that requirement within the framework of the process-based approach to information security that this research suggests is recognised industry practice;
- The references to standards such as ISO 27001 and ISO 27002 in the reports suggest that the authors of the report may not be truly conversant with the intended operation of those standards, either alone or as part of an overarching management system;
- There are few references in the OMI reports to the OAIC's own guidance and no reference to other case notes or OMI reports that might be expected to be of some relevance.

Based on these findings, it is difficult to interpret any of the 6 reports as materially supporting the adoption of organisational information security practices aligned to industry practice.

Issues regarding the transparent, balanced and vigorous use by the Commissioner of investigation powers include:

- The selection of incidents to investigate does not appear to be balanced, as the same single criterion was used for the selection of all 6 cases for investigation;
- The investigation process itself appears to be neither balanced nor vigorous. Reliance is placed almost entirely on the responses provided by the organisations being investigated, with very little engagement in regard to that information and little detailed questioning;
- The investigation files suggest that the OAIC does not have the number of resources or the specialist skilled staff required to carry out investigations into cases that involve complex technology systems. This in turn suggests that the investigations are not conducted with the vigour which might otherwise be expected;
- The lack of clear links between the findings of facts and the reasons for reaching a particular decision in all the investigations other than Vodafone means there is limited transparency of decision-making provided by the OMI reports;
- The absence of any reference to the standard used by the OAIC in arriving at its decision in regard to whether 'reasonable steps' had been taken for the purposes of NPP 4 also affects the transparency of decision-making;
- There is almost no transparency in terms of the application of the Commissioner's own guidance to the circumstances of the different investigations;
- The decision to publish the reports may not be regarded as balanced, seemingly being motivated by the need to reassure the public in response to media reports, rather than supporting other regulatory outcomes, such as

providing examples of the OAIC's application of or interpretation of the privacy principles or addressing a systemic issue;[1196] and

- The investigation files show issues, in some cases, with the timeliness of informing respondents of the outcomes of investigations and the decision to publish a report. The Medvet case is particularly concerning, given the change in decision by the Commissioner after a Close Letter and draft OMI report had been sent to the respondent.

The Commissioner's failure to exercise the available powers in a fully transparent, balanced and vigorous way means that in practice the regulatory system is not functioning in accordance with the assumptions made regarding the effective operations of the two regulatory foundations underpinning the *Privacy Act*: principle-based regulation and a responsive regulatory approach to compliance.

As discussed in Chapter 2, PBR requires a closely engaged regulator using a responsive enforcement approach to achieve clearly communicated outcomes and goals. There is little evidence of this from the Commissioner's use of its oversight and investigation powers in relation to NPP 4. The interactions considered in this research could not be characterised as any sort of ongoing engagement between the OAIC and any sector or industry group in conversations or dialogue of any sort regarding the purpose or application of NPP 4. The use of the oversight powers is limited, high-level, reactive and largely one-sided. The use of the investigation powers is necessarily more inclusive of input from the regulated community but the published outcomes and the associated media engagement could not be regarded as any sort of 'regulatory conversation.' One of the particular outcomes noted in this research is the lack of transparency of decision-making in the published reports.

---

[1196] The draft Regulatory Powers Policy refers to instilling public confidence as part of the OAIC's main goal to promote and ensure the protection of personal information, which accords with the conclusion reached by this research that the main reason for publishing OMI reports is community reassurance rather than transparency of decision making or the provision of guidance or education, see *Regulatory Powers Policy, above n 227*.

Those reports do not work as a body of decisions to show the development and application of principles on which the Commissioner bases its interpretation of NPP 4 (or NPP 2) in different fact circumstances. This means that the regulated community, as well as scholars, privacy experts and advisers, have little basis for a critical analysis of how the Commissioner is interpreting the Act.[1197]

In theory, principles shift the responsibility for ensuring that the objectives of the principles are met from the regulator to the regulated, which in turn means that regulators must focus on the internal systems of management and control implemented by the regulated community.[1198] The failure to recognise and apply an industry best practice approach to security suggests that the Commissioner may not in fact be able or willing to involve itself in overseeing the internal information security management systems that is required in a substantive PBR system. Even assuming that the OAIC did have the requisite skills and understanding in regard to information security management systems, it is difficult to see how the Commissioner would be able to regulate the operation of these internal systems in the way contemplated by PBR and a compliance-based approach, with the limited resources available. As noted in Chapter 9.7, resource issues are responsible for the 'on the papers' approach to investigations undertaken by the OAIC and have also resulted in a reduction in:

- The number of audits undertaken;
- The timeliness of responding to complaints;
- The number of case notes published; and
- The number of own motion investigations opened.

In 2014, the Commissioner said '[e]mbedding change and best practice successfully into organisations and agencies that are entrusted with the personal information of the community must be what we are aiming for' and confirmed that the OAIC would remain keen to work with all entities to achieve this through the

---

[1197] See the earlier discussion of the problems with providing inadequate reasons for decisions in Chapter 2.6.1.

[1198] Black, above n 180, 7.

coming year.[1199] However, to date, the Commissioner's exercise of its oversight and investigation powers in relation to NPP 4 has contributed little to embed an industry standard approach to information security.

It may be that PBR coupled with a compliance regulatory approach is the best regulatory system for the protection of personal information and the resolution of competing rights that are often implicit in privacy issues. However, it is not clear that this regulatory system when considered in the context of the resources and skills available to the OAIC is best suited to supporting the adoption of better security practices by Australian organisations.

## 11.1 THE FUTURE

From March 2014, NPP 4 is replaced by APP 11. One of the changes made in the new principle is the replacement of the term 'reasonable steps' with 'such steps as are reasonable in the circumstances.' The Explanatory Memorandum provides that this change is to make it clear that the assessment is an objective one albeit that 'when considering what are objectively reasonable steps the specific circumstances of each case must be considered.'[1200] It may be that this change in wording will direct the Commissioner's enquires towards a more detailed consideration of the specific circumstances of each case. Such consideration may then be reflected in a more transparent process of decision-making, where the specific circumstances are part of the findings of fact on which material findings are made to support decisions.

More importantly perhaps, the Commissioner's powers have been extended.

From March 2014 the OAIC may conduct privacy performance assessments on the levels of compliance of private entities well as public entities.[1201] However, given the limited use of the Commissioner's assessment powers to date as discussed in Chapter 5 it is doubtful whether, in the absence of significant resourcing increases,

---

1199 Timothy Pilgrim, Privacy Commissioner, 'Privacy and Transparency' (Presentation to the Privacy Awareness Week 'Up close and personal' business breakfast, 5 May 2014) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-and-transparency>.

1200 *Explanatory Memorandum*, n 122, 54.

1201 *Privacy Act* s 33C.

this new power will be used any more extensively in regard to private entities. It is also unclear whether any of the issues identified in the Commissioner's use of its audit powers in relation to public entities will be remedied.

Also as of March 2014, the Commissioner has the benefit of additional investigation and enforcement powers that may be used in relation to APP 11. These powers include the power to:

- Make a determination following an own motion investigation;[1202] and
- Accept written enforceable undertakings by entities to take, or refrain from taking, specified actions to ensure compliance with the *Privacy Act*.[1203]

In the interview with the Assistant Commissioner Compliance, she referred to these additional powers, commenting that they bring a 'heightened deterrent and educative element to those matters.'[1204]

As already discussed,[1205] prior to March 2014, the Commissioner did not have the power to make any determination at the conclusion of an own motion investigation. This is one of the factors thought to have influenced the conciliatory approach taken to investigations by the Commissioner and the interest shown by the Commissioner in being able to conclude investigations on the basis of outcomes agreed with the respondent.[1206] Without recourse to more punitive powers, such as the ability to issue a determination with adverse findings, there has been little that the Commissioner could do if confronted by an uncooperative or recalcitrant respondent in an OMI.[1207]

---

1202 *Privacy Act* s 52(IA).

1203 Ibid s 33E.

1204 Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012)

1205 See Sections 7.2 and 7.3.

1206 O'Connor, above n 65; see also Interview with Assistant Commissioner Compliance (Sydney, 14 December 2012),

1207 The OPC acknowledged that it had 'experienced some difficulties' in dealing with potential privacy breaches where there was no individual complainant and where the respondent was not cooperative. See *Getting in on the Act*, above n 155, 155 and *For your information*, above n 32, [50.7].

Another change effective as of March 2014 may have implications for the Commissioner's use of its investigation powers. Determinations will now be subject to merit reviews by the Administrative Appeals Tribunal (not limited to grounds of procedural fairness or a question of law).[1208] The possibility of an own motion investigation culminating in the making of a reviewable determination may change the nature of the investigation undertaken and the content of any report issued, bearing in mind the potential appeal and review rights.[1209] It any case, where the Commissioner does make a determination, the respondent has the right to be provided with the reasons for the decision, which should include findings on material questions of fact that refer to the evidence or other material on which those findings were based.[1210] Where this occurs, it is likely to improve the transparency of the Commissioner's reporting.

On its face, this extension of the determination power to investigations commenced on the Commissioner's own motion would seem to be a significant addition to the Commissioner's armoury. However, it is not clear that the Commissioner will use this new power to make a determination following an OMI. As discussed, the Commissioner has to date issued few determinations.[1211] The Commissioner has recently referred to its intention to issue more determinations, referring specifically to the value of determinations in explaining the Commissioner's interpretation of the privacy principles.[1212] Perhaps reflecting this new intention, six new determinations have been issued from March 2014, making a

---

1208 *Privacy Act* s 96(1)(c).

1209 Pursuant to Privacy Act s 96(1)(c) determinations will now be subject to merit reviews by the Administrative Appeals Tribunal. See also Ofice of the Australian Information Commissioner, 'Privacy review rights' (1 September 2009) < http://www.oaic.gov.au/privacy/privacy-review-rights>.The same reasoning may apply to the potential use by the Commissioner of the power to seek a penalty, by application to the Federal Court; *Privacy Act* Pt IVB.

1210 *Privacy Act* s 52. See also *Administrative Appeals Tribunal Act 1975* (Cth) s 28.

1211 See Section 7.3.

1212 Timothy Pilgrim, Privacy Commissioner 'Privacy law reform: challenges and opportunities' (Presentation to Emerging Challenges in Privacy Law Conference, 23 February 2012) <http://www.oaic.gov.au/news/speeches/timothy_pilgrim/timothy_pilgrim_emerging_challenges_feb12.html#_ftn1>.

total of 16 determinations.[1213] This heightened recent activity may indicate a new resolve to make determinations, including as an outcome of own motion investigations. Whether or not there will be more determinations made generally or in regard to cases which raise questions of data security is not clear, as the issues that some have regarded as impacting on the Commissioner's use of the determination power (including the Federal Court right to hear any enforcement action by way of a hearing de novo and the absence of any right for a complainant to require that a determination be made) remain.[1214]

Given the Commissioner's historical reluctance to make determinations and the continued relevance of the factors thought to influence that reluctance it seems more likely that the Commissioner will elect to take an alternative approach to concluding own motion investigations and, instead of making a determination, will seek to secure an enforceable undertaking from respondents.[1215] As the Commissioner has previously concluded a number of investigations based on undertakings made by the respondent this seems likely to be a more attractive resolution than making a determination. [1216] If this is the avenue pursued by the Commissioner it is unlikely to contribute greatly to either the jurisprudence or even the more general understanding of the Commissioner's interpretation and application of APP 11. Enforceable undertakings are, by their nature, enforceable without any judicial review or other consideration of the merits of the undertaking. This means that the conduct and outcome of those investigations which culminate in an enforceable undertaking will not be subject to any form of judicial review. Enforceable undertakings could be

---

1213 Prior to 2011, there were eight determination, the last issued in 2004. The eight determinations issued from 2011 to February 2015 are *'EQ' and Great Barrier Reef Marine Park Authority* [2015] AICmr 11; *'DO' and Department of Veterans' Affairs* [2014] AICmr 124; *'DK' and Telstra Corporation Limited* [2014] AICmr 118; *'CP' and Department of Defence* [2014] AICmr 88); 'CM' and Corporation of the Synod of the Diocese of Brisbane [2014] AICmr 86 *'BO' and AeroCare Pty Ltd* [2014] AICmr 32; *'S' and Veda Advantage Information Services and Solutions Limited* [2012] AICmr 33 ; *'D' and Wentworthville Leagues Club* [2011] AICmr 9.

1214 See Section 7.3 and the discussion of some of the reasons for the low number of determinations..

1215 *Privacy Act* s 33E.

1216 In both the Vodafone and the Telstra Bundles investigations the respondents gave undertakings to the Commissioner to take agreed remediation steps and report back to the Commissioner on the action that had been taken.

compared to conciliated outcomes: they are the agreement reached between the regulator and the respondent as to the appropriate remediation action to be taken to enable the regulator to close an investigation. Although of some use in terms of providing reassurance that identified problems may be addressed, the contents of enforceable undertakings will not have any significant weight in terms of the interpretation or application of APP 11. Similarly, the published reports about investigations that culminate in enforceable undertakings are unlikely to be significantly different to the reports considered in this research, with the attendant issues of transparency, balance and vigour and inconsistency with industry practice.

In March 2014 the OAIC released a draft Regulatory Powers Policy[1217] for public consultation. The Regulatory Powers Policy is intended to explain the OAIC's goals of taking privacy regulatory action, the guiding principles to be used and how the OAIC decides whether to take regulatory action in a particular circumstance. The Policy reaffirms the OAIC's commitment to the Ayres and Braithwaite compliance approach, stating its preferred regulatory approach is to encourage voluntary compliance and to work with entities to ensure best privacy practice and prevent privacy breaches.[1218] The draft Policy also refers to a number of general principles that should guide its regulatory decisions and actions, including independence, proportionality, consistency, timeliness and transparency about how it intends to use its privacy regulatory powers, and about the regulatory outcomes it has achieved.[1219] These principles are broadly consistent with the principles of transparency, balance and vigour which have been used in this research.

If the Commissioner issues a final *Regulatory Powers Policy* in similar terms to the draft, it is difficult to see how the Commissioner will be able to comply with these principles if it continues to exercise its powers in relation to the Security Principle in the same manner as considered in this research. This will certainly be the case if the OAIC is not provided with access to additional resources and increased skills to support the exercise of the oversight and enforcement powers in relation to

---

1217 *Regulatory Powers Policy*, above n 227.

1218 Ibid, [3].

1219 Ibid, [13].

complex information security cases. However, in view of the proposal to re-structure the OAIC, it seems likely that the Commissioner's current resource and skills issues will become more acute.[1220]

Similarly, it is difficult to see how the Commissioner's expanded powers could be exercised in a more transparent, balanced and vigorous way to support the adoption of an industry best practice approach to information security, without the resources and skills to draft appropriate general guidance, proactively monitor compliance, carry out investigations that will meet principles of procedural fairness and publish investigation reports that provide true transparency of the Commissioner's decision-making process, as well as support for an industry practice approach to information security. One option may be the establishment of expert panels that could be consulted on the implications of technological developments for data security or be used to develop education and guidance materials,[1221] which would also be consistent with the encouragement provided by the ALRC to the growth of 'compliance professionals' and closer engagement with the regulated community.[1222]

If the Australian government is committed to the use of PBR and a responsive regulatory approach as the regulatory models for privacy and the protection of personal information, it should also ensure that the regulator has the resources and skills to support the proper implementation of the principles. Until such time as the Commissioner is able to exercise its powers in the complex ways contemplated by the regulatory foundations of the *Privacy Act*, it is unlikely that the OAIC's use of its powers in regard to the Security Principle will result in any significant improvement to the security of the personal information held by Australian organisations.

---

1220 See, eg, Bruce Arnold, 'Ending the OAIC and new frameworks for privacy law' (2014) 11(5) *Privacy Law Bulletin* 66. See also the references in n 133.

1221 *For your information*, above n 32, Recommendation 28–3, 951. The right for the Commissioner to appoint expert panels is now included in *Privacy Act* s 27(3).

1222 Ibid [4.65] – [4.68].

# Appendices

**Appendix A**
**OAIC and OPC case notes Published from 2008 – 2014[1223]**

| Year | Name of case note |
|---|---|
| 2013 - 2014 | [None published] |
| 2012 - 2013 | [None published] |
| 2011 - 2012 | 1. A and Financial Institution [2012] AICmrCN 1 (1 May 2012),<br>2. H and Registered Club [2011] AICmrCN 2 (22 December 2011),<br>3. K and Finance Company [2011] AICmrCN 5 (22 December 2011),<br>4. M and Law Firm [2011] AICmrCN 7 (22 December 2011)<br>5. O and Professional Association [2011] AICmrCN 9 (22 December 2011)<br>6. P and Retail Company [2011] AICmrCN 10 (22 December 2011)<br>7. Q and Financial Institution [2011] AICmrCN 11 (22 December 2011),<br>8. R and Credit Reporting Agency [2011] AICmrCN 12 (22 December 2011), |
| 2010 - 2011 | 1. A v Credit Provider [2011] PrivCmrA 1 (3 May 2011),<br>2. B v Law Firm [2011] PrivCmrA 2 (3 May 2011),<br>3. C v Charity [2011] PrivCmrA 3 (3 May 2011), |

[1223] This list is complete as at 1 September, 2014.

| | |
|---|---|
| | 4. D v Charitable Organisation [2011] PrivCmrA 4 (3 May 2011),<br>5. E v Insurance Company [2011] PrivCmrA 5 (3 May 2011),<br>6. F v Contract Service Provider to a Commonwealth Government Agency [2011] PrivCmrA 6 (3 May 2011),<br>7. H v Health Service Provider [2010] PrivCmrA 9 (24 December 2010),<br>8. I v Commonwealth Agency [2010] PrivCmrA 10 (24 December 2010),<br>9. J v Credit Reporting Agency [2010] PrivCmrA 11 (24 December 2010),<br>10. K v Commonwealth Agency [2010] PrivCmrA 13 (24 December 2010),<br>11. L v Commonwealth Agency [2010] PrivCmrA 14 (24 December 2010),<br>12. M v Body Corporate [2010] PrivCmrA 15 (24 December 2010),<br>13. N v Restaurant [2010] PrivCmrA 17 (24 December 2010),<br>14. v Financial Institution [2010] PrivCmrA 18 (24 December 2010),<br>15. P v Insurer [2010] PrivCmrA 19 (24 December 2010),<br>16. Q v Law Firm [2010] PrivCmrA 20 (24 December 2010),<br>17. R v Retailer [2010] PrivCmrA 21 (24 December 2010),<br>18. S v Debt Collector [2010] PrivCmrA 22 (24 December 2010),<br>19. T v Investment Services Provider [2010] PrivCmrA 23 (24 December 2010). |
| | 1. F v Medical Specialist [2009] PrivCmrA 8 (31 August 2009), |

| | |
|---|---|
| 2009 – 2010 | 2. G v Counselling Service [2009] PrivCmrA 9 (31 August 2009),<br>3. H v Telecommunications Company [2009] PrivCmrA 10 (31 August 2009),<br>4. I v Insurance Company [2009] PrivCmrA 11 (31 August 2009),<br>5. J v Commonwealth Agency [2009] PrivCmrA 13 (19 November 2009),<br>6. K v Commonwealth Agency [2009] PrivCmrA 14 (19 November 2009),<br>7. L v Health Service Provider [2009] PrivCmrA 15 (19 November 2009),<br>8. M v Financial Institution [2009] PrivCmrA 16 (19 November 2009),<br>9. N v Commonwealth Agency [2009] PrivCmrA 17 (19 November 2009),<br>10. v Automotive Company [2009] PrivCmrA 18 (22 December 2009),<br>11. P v Commonwealth Agency [2009] PrivCmrA 19 (22 December 2009),<br>12. Q v Credit Provider [2009] PrivCmrA 20 (22 December 2009),<br>13. R v Company [2009] PrivCmrA 21 (22 December 2009),<br>14. S v Debt Collection Agency [2009] PrivCmrA 22 (22 December 2009),<br>15. T v Commonwealth Agency [2009] PrivCmrA 23 (22 December 2009),<br>16. U v Telecommunications Company [2009] PrivCmrA 24 (22 December 2009), |

| | |
|---|---|
| | 17. A v Private Health Service Provider [2010] PrivCmrA 2 (31 May 2010),<br>18. B v Charity Organisation [2010] PrivCmrA 3 (31 May 2010),<br>19. C v Telecommunications Company [2010] PrivCmrA 4 (31 May 2010),<br>20. D v Commonwealth Agency [2010] PrivCmrA 5 (31 May 2010),<br>21. E v Private School [2010] PrivCmrA 6 (31 May 2010),<br>22. F v Health Service Provider [2010] PrivCmrA 7 (31 May 2010),<br>23. G v Finance Company [2010] PrivCmrA 8 (31 May 2010) |
| 2008 - 2009 | 1. S v Health Service Provider [2008] PrivCmrA 19 (29 August 2008),<br>2. T v Private Community Centre [2008] PrivCmrA 20 (29 August 2008),<br>3. U v Betting Agency [2008] PrivCmrA 21 (29 August 2008), V Commonwealth Agency [2008] PrivCmrA 22 (5 December 2008), W v Pathology Clinic [2008] PrivCmrA 24 (5 December 2008),<br>4. A v Medical Practitioner [2009] PrivCmrA 1 (5 May 2009),<br>5. B v Cleaning Company [2009] PrivCmrA 2 (5 May 2009),<br>6. C v Commonwealth Agency [2009] PrivCmrA 3 (5 May 2009),<br>7. D v Finance Company [2009] PrivCmrA 4 (5 May 2009),<br>8. E v Advertiser [2009] PrivCmrA 5 (5 May 2009) |

**Appendix B**
**OAIC and OPC OMI reports Published from 2007 – 2014[1224]**

| Year | Name of OMI report |
|---|---|
| 2013 - 2014 | 1. Pound Road Medical Centre: Own motion investigation report (July 2014)<br>2. Cupid Media: Own motion investigation report(June 2014)<br>3. Multicard Pty Ltd: Own motion investigation report (May 2014)<br>4. Telstra Corporation Limited (Telstra): Own motion investigation report (March 2014)<br>5. AAPT and Melbourne IT: Own Motion Investigation Report (October 2013) |
| 2012 - 2013 | 1. Medvet Science Pty Ltd: Own motion investigation report (July 2012),<br>2. Dell Australia and Epsilon: Own motion investigation report (July 2012) |
| 2011 - 2012 | 1. Sony PlayStation Network / Qriocity: Own motion investigation report (September 2011)<br>2. Telstra Corporation Limited: Own motion investigation report (June 2012),<br>3. First State Super Trustee Corporation: Own motion investigation report (June 2012)<br>4. Telstra Corporation Limited (Telstra): Own motion investigation report (July 2011) |
| 2010 - 2011 | 1. Vodafone Hutchison Australia: Own motion investigation |

[1224] This list is complete as at 1 September, 2014.

| | |
|---|---|
| | report (February 2011)<br>2. Professional Services Review Agency: Own motion investigation report (December 2010),<br>3. Own Motion Investigation v Telecommunications Company [2010] PrivCmrA 16 (24 December 2010),<br>4. Own Motion Investigation v Information Technology Company [2010] PrivCmrA 24 (24 December 2010),<br>5. Own Motion Investigation v Airline [2010] PrivCmrA 12 (24 December 2010), |
| 2009 - 2010 | 1. Own Motion Investigation v Insurance Company [2010] PrivCmr 1 |
| 2008 - 2009 | 2. Own Motion Investigation v Airline [2009] PrivCmr 7<br>3. Own Motion Investigation v Medical Centre [2009] PrivCmr 6<br>4. Own Motion Investigation v Retailer [2009] PrivCmrA 25 |
| 2007 - 2008 | 1. Own Motion Investigation v Direct Marketer [2008] PrivCmrA 23 |

## Appendix C
## Investigation Records from OMI Files

**Telstra Mail Out:**

1. RFI Letter: Letter from Timothy Pilgrim to Ms Helen Lewin, Telstra entitled 'Own Motion Investigation', 28 October 2010;
2. Close Letter: Letter from Mark Hummerston to Ms Helen Lewin entitled 'Own motion investigation – mailing list incident' 16 May 2011; and
3. Email thread between Helen Lewin, Telstra and OAIC including email to Timothy Pilgrim, 26 May 2011.

**Vodafone**

1. RFI Letter: Letter from Timothy Pilgrim OAIC to Vodafone, 10 January 2011 Vodafone Schedule B Document 14; and
2. Letter from Timothy Pilgrim OAIC to Vodafone 16 February 2011, Vodafone Schedule A Document 5.

**Sony**

1. RFI Letter: Letter from Timothy Pilgrim to Sony's Managing Director dated 27 April 2011, Sony Schedule B Document 5; and
2. Email from Roger Clarke to privacy@lists.efa.org.au, 4 May 2011, Sony Schedule B Document 15.

**Dell Epsilon**

1. RFI Letter from Mark Hummerston (OAIC) to Dell, 19 April 2011 Dell Schedule A Document 9
2. Email threader, with header email from MH (OAIC) to MS re Dell response to OMI (Dell response is attached) 11 May 2011, 2011 Dell Schedule A Document 7;
3. Email from Dell to MS (OAIC) re status of audit, 19 July 2011 Dell Schedule A Document 2;
4. 1 page excerpt setting out relationship of NPP 2 and NPP 4, email dated 24 May 2012, Dell Schedule B Document 2;

5. CMS Report Epsilon Investigation File, Epsilon Redacted Documents Document 1; and
6. Letter from Mark Hummerston (OAIC) to Dell: Advising decision to cease investigation, 11 January 2012, Dell Schedule A Document 10.

**Telstra Bundles**

1. RFI Letter: Letter from Mark Hummerston, Assistant Commissioner Compliance to Telstra dated 12 December, 2012 Telstra Schedule B Document 60;
2. Letter from Mark Hummerston, Assistant Commissioner Compliance to Telstra dated 8 March 2012. Telstra Schedule B Document 40; and
3. Email thread between OAIC and Telstra dated 15 March 2012. Telstra Schedule B Document 35.

**Medvet**

1. RF Letter: Letter from Timothy Pilgrim to Medvet re OMI against Medvet, 20 July 2011 Medvet Schedule B Document 21;
2. CMS File note, 11 October 2011;
3. Close Letter: Letter from Mark Hummerston, Assistant Commissioner, OAIC to CEO Medvet, 19 December, 2011 (Medvet Schedule A Document 1); and
4. Letter from Timothy Pilgrim to Medvet re OMI outcome, 10 July 2012. Medvet Schedule B Document 3.

Attachment G.pdf

## Appendix D
## State Privacy Laws

*Privacy and Personal Information Protection Act* 1997 (NSW)

*Health Records and Information Privacy Act* 2002 (NSW)

*Information Privacy Act* 2009 (Qld)

*Information Privacy Act* 2000 (Vic)

*Health Records Act* 2001 (Vic)

*Information Protection Act* 2002 (NT)

*Personal Information Protection Act* 2004 (Tas)

## Appendix E
## Case notes and OMI reports Relating to NPP 4

**case notes**

*E v Financial Institution* [2003] PrivCmrA 3

*N v Internet Service Provider* [2004] PrivCmrA 10

*J v Superannuation Provider* [2005] PrivCmrA 7

*R v Internet Service Provider* [2005] PrivCmrA 17

*I v Retail Company* [2006] PrivCmrA

*N v Utility Provider* [2006] PrivCmrA 13

*Q v Financial Institution* [2006] PrivCmrA 16

*U v Banking Institution* [2006] PrivCmrA 20

*V v Health Service Provider* [2006] PrivCmrA 21

*D v Insurance Company* [2007] PrivCmrA 6

*E v Retail Organisation* [2007] PrivCmrA 7

*H v Health Service Provider* [2007] PrivCmrA 10

*I v Insurance Company* [2007] PrivCmrA 11

*R v Retailer* [2007] PrivCmrA 20

*X v Transport Company* [2007] PrivCmrA 26

*Y v Ticketing Company* [2007] PrivCmrA 27

*D v Health Service Provider* [2008] PrivCmrA 4

*P v Private Health Service Provider* [2008] PrivCmrA 16

*S v Health Service Provider* [2008] PrivCmrA 19

*G v Counselling Service* [2009] PrivCmrA 9

*M v Body Corporate* [2010] PrivCmrA 15

*G v Parking Services Organisation* [2011] AICmrCN 1

*H v Registered Club* [2011] AICmrCN 2

**Own Motion Investigations**

*OPC v Banking Institution* [2005] PrivCmrA 11

*Own Motion Investigation v Bankrupt Trustee Firm* [*2007*] PrivCmrA 5

*Own Motion Investigation v Direct Marketer* [2008] PrivCmrA 23

*Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6

*Own Motion Investigation v Retailer* [2009] PrivCmrA 25

*Own Motion Investigation v Airline* [2010] PrivCmrA 12

*Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16

*Own Motion Investigation v Information Technology Company* [2010] PrivCmrA 24

**Appendix F**
**Interview Guide**

| **General Question** |
| --- |
| Could you tell me a little about your professional life so far? What did you do before coming to the OAIC? |
| **Background** |
| Could you tell me about how the OAIC operates in regard to its Privacy functions? |
| Could you describe for me your role – in particular your different functions: e.g. guidance, advisory, monitoring and investigations?<br><br>How is each of those discharged? |
| What are your strategic objectives and any KPIs (across all functions) |
| Could you tell me generally about how the investigation process usually works within OAIC?<br><br>Have there been any changes in that approach over the last few years? |
| Does the OAIC review the exercise of its investigatory powers? |
| **Establishing the Framework of the Investigation** |
| Can you tell me generally how you approach cases involving an alleged breach of NPP 4?<br><br>Does the approach differ depending on whether there has also been an unauthorised disclosure of personal information? |
| I would like to talk mostly about the most recent Own Motion Investigations involving NPP 4.<br><br>What were the main reasons for deciding to open Own Motion Investigations in these cases?<br><br>Does the investigation approach change in the case of Own Motion Investigations? |

| |
|---|
| Investigations can be categorised as 'evidence focused' or 'outcome focused.'[1225]<br><br>How would you categorise these investigations? |
| **The Investigation** |
| Can you take me through the role you played in each of these cases e.g. Did you review the investigation plans? |
| What input did you have to the gathering of evidence? |
| Do you know what standard of proof was used in these investigations?<br><br>How was that applied to the evidence gathered in these investigations? |
| **Determining Investigation Outcomes & Reporting** |
| How was the final conclusion reached in each case?<br><br>What contact was had with the other side as part of that process? |
| A report of each investigation was prepared. Who was responsible for writing the report, who approved it and what happened prior to its publication? |
| A report of this investigation was published. Who made the decision to publish the report? Why was this report published? What contact was had with the other side in regard to the publication of the report? |
| The report refers to [indicate any undertaking made by the other party]. Can you tell me what has happened in regard to those undertakings? |
| **Reflections on Investigation** |
| Do you have any reflections on any of these investigations? |

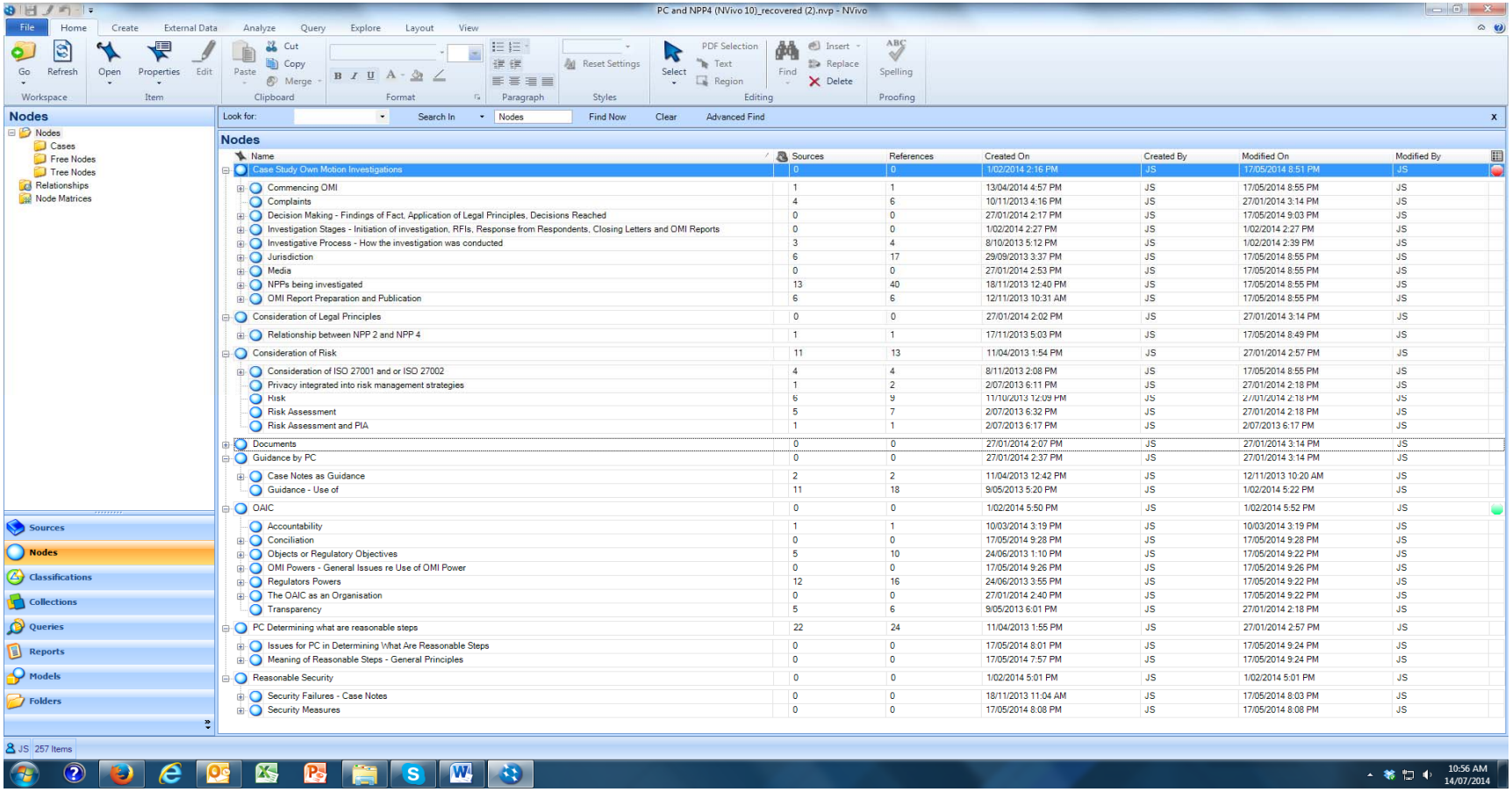
[1225] NSW Ombudsman Guide to Investigating Complaints 2004 p15 - 16

| |
|---|
| The proposed amendments to the *Privacy Act* give the Commissioner some additional powers. Do you think that, if those powers had been available, there would have been a different outcome? |
| Were there any other outcomes from this investigation that you can think of? |
| A number of the investigations raised jurisdictional issues which seemed to add complexity to the investigation. Would you be able to talk about that? |
| The Privacy Commissioner has recently undertaken significantly more OMIs than in the past. Could you tell me about that (as a compliance approach) |
| The Privacy Commissioner has indicated a greater willingness to pursue organisations that fail to meet their obligations to secure personal information. Can you tell me more about that? |
| There has been a reduction in the number of published case notes so far in 2012. Do you have any comments on that? |
| **Conclusion** |
| Is there anything else that you would like to add about any of the things we've covered today? Or anything else that might be relevant to this research? |
| Do you have any questions for me? |

## Appendix G
## Type of Records - Investigation Files

| Type of Record | Medvet | Telstra Bundle | Dell/ Epsilon | Sony | Voda fone | Telstra Mail Out | TOTAL |
|---|---|---|---|---|---|---|---|
| External Email (to or from OAIC) | 8 | 17 | 12 | 13 | 6 | 4 | **60** |
| Internal Email (w/I OAIC) | 5 | 3 | 9 | 6 | 8 | 0 | **31** |
| Letter | 9 | 4 | 10 | 6 | 9 | 5 | **43** |
| Phone Call | 7 | 3 | 3 | 7 | 1 | 1 | **22** |
| Meeting with Respondent | 0 | 2 | 0 | 0 | 1 | 0 | **3** |
| Internal Meeting | 3 | 2 | 2 | 4 | 0 | 0 | **11** |
| Admin task | 14 | 28 | 11 | 10 | 2 | 0 | **65** |
| Press | 2 | 0 | 5 | 8 | 8 | 0 | **23** |
| Media Release | 0 | 1 | 1 | 0 | 2 | 0 | **4** |
| OMI report | 1 | 1 | 0 | 1 | 2 | 0 | **5** |
| External (Third Party)Report | 2 | 0 | 2 | 0 | 0 | 0 | **4** |
| Duplicate | 0 | 4 | 2 | 0 | 0 | 0 | **6** |

# Appendix H
# Qualitative Analysis –nVivo Coding



**Appendix I**
**OAIC Submissions Made in 2013 – 2014**

http://www.oaic.gov.au/news-and-events/submissions/

| | |
|---|---|
| Submission to the ALRC on Discussion Paper 80: Serious invasions of privacy in the digital era | June 2014 |
| Notification of employment decisions in the Gazette – a discussion paper | May 2014 |
| Submission to the Senate regarding the TIA inquiry | March 2014 |
| Submission on the Review of the AML/CTF regime | February 2014 |
| Whois policy review for the .au domain | February 2014 |
| Serious Invasions of Privacy in the Digital Era | December 2013 |
| Queensland Government Review of the Information *Privacy Act* 2009 and Right to Information Act 2009 | November 2013 |
| Internet Corporation for Assigned Names and Numbers Study of Whois Privacy and Proxy Service Abuse | November 2013 |
| Submission to NHMRC re proposed amendments to chapter 2.3 of the National Statement | August 2013 |
| Review of Subdivision A of Division 6 of Part VIIC of the Crimes Act 1914 — the working with children exclusion | July 2013 |

## Appendix J OAIC Privacy Speeches 2011 – 2014

| | |
|---|---|
| 2013 - 2014 | Timothy Pilgrim, Privacy Commissioner 'Defining the sensor society' Presentation to the 'Defining the Sensor Society Conference' at University of Queensland, Brisbane, 8 May, 2014 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/defining-the-sensor-society><br><br>Timothy Pilgrim, Privacy Commissioner 'Privacy matters', Presentation to the 'Privacy matters' public lecture at Griffith University, Brisbane, 8 May 2014 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-matters>.<br><br>Timothy Pilgrim, Privacy Commissioner, 'Mapping data breach notification' Presentation at iappANZ data breach panel discussion, Sydney, 6 May 2014 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/mapping-data-breach-notification>.<br><br>Professor John McMillan, Australian Information Commissioner, 'Up Close and Personal' Presentation to the Privacy Awareness Week 'Up close and personal' business breakfast, 5 May 2014, < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/up-close-and-personal><br><br>Timothy Pilgrim, Australian Privacy Commissioner "Privacy and Transparency" Presentation to the Privacy Awareness Week 'Up close and personal' business breakfast, 5 May 2014 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-and-transparency><br><br>Timothy Pilgrim, Privacy Commissioner, 'Credit Reporting Changes' Presentation to the Australian Retail Credit Association 'New era of credit' forum, Sydney, 18 March 2014, < http://www.oaic.gov.au/news-and-events/speeches/privacy- |

| | |
|---|---|
| | speeches/credit-reporting-changes><br><br>Timothy Pilgrim, Privacy Commissioner 'Privacy Reform – Act Three' Presentation to the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>.<br><br>John McMillan, Australian Information Commissioner 'Developing Tools for Global Privacy Compliance' Presentation to panel session at the 35th International Conference of Data Protection and Privacy Commissioners, Warsaw, 23-26 September 2013, < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/developing-tools-for-global-privacy-compliance> |
| 2012 - 2013 | Timothy Pilgrim, Privacy Commissioner 'Setting the scene – Privacy law in Australia', Presentation to the Australian Communications and Media Authority's Citizens Conversation series, Sydney, 25 June 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/setting-the-scene-privacy-law-in-australia><br><br>Timothy Pilgrim, Australian Privacy Commissioner "Privacy law reform — Get in on the Act" Presentation at the iappANZ Privacy Awareness Week seminar, Brisbane, 1 May 2013 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-law-reform-get-in-on-the-act><br><br>Timothy Pilgrim, Privacy Commissioner 'Privacy Awareness Week 2013 Privacy Commissioner's Update' Presentation to Privacy Awareness Week 2013 Business Breakfast, 29 April 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-awareness-week-privacy-commissioner-s-update><br><br>Timothy Pilgrim, Australian Privacy Commissioner 'Privacy Update' Presentation to |

| | |
|---|---|
| | Australian Corporate Lawyers Association South Australian corporate counsel day, Adelaide Convention Centre, Friday 22 March 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-update><br><br>Timothy Pilgrim, Privacy Commissioner, 'Update your privacy settings' Presentation to the Communications and Media Law Association, Sydney, 7 March 2013 < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/update-your-privacy-settings> |

## Appendix K
## OAIC Audit Reports

### OAIC Audit Reports Published Between November 2010 – June 2014[1226]

| | Title of Report | Date Report Issued | IPP 4 in Scope |
|---|---|---|---|
| 1 | Healthcare Identifiers Service: Audit report | June 2014 | No |
| 2 | Calvary Private Hospital ACT: Assessment report | June 2014 | No |
| 3 | Healthcare Identifiers Service — Department of Human Services: Audit report | April 2014 | No |
| 4 | Collection and security of student personal information – Canberra Institute of Technology: Audit report | April 2014 | Yes |
| 5 | Collection and Requests for Student Information: Audit report | December 2013 | No |
| 6 | Public Transport Systems: MyWay audit | June 2013 | Yes |
| 7 | Requests for Information for Passenger Name Record Data - Australian Customs and Border Protection Service Audit Report | June 2013 | Yes |
| 8 | National Document Verification Service - Department of Foreign Affairs and Trade - Audit Report 2012 | December 2012 | Yes |

[1226] OAIC 'Privacy Assessments' http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-assessments.

| | | | |
|---|---|---|---|
| 9 | Healthcare Identifiers Service - Department of Human Services - Audit Report | August 2012 | Yes |
| 10 | Passenger Name Records (PNR data) Australian Customs and Border Protection Service Audit Report | July 2012 | Yes |
| 11 | ACT – Department of Disability, Housing and Community Services, The Office for Children, Youth and Family Support Audit Report | July 2011 | Yes |
| 12 | Healthcare Identifiers Service - Medicare Australia Audit Report | July 2011 | Yes |
| 13 | Australian Federal Police (ACT Policing Branch) Audit Report | July 2011 | Yes |
| 14 | National Document Verification Service, Centrelink - Audit Report | June 2011 | Yes |

**OAIC Audit Reports Published Between March 2004 - October 2010**[1227]

| | **Title of Report** | **Date Report Issued** | **IPP 4 in Scope** |
|---|---|---|---|
| 15 | ACT Residential Tenancies Tribunal: Client and Employee Records audit | May 2004 | Yes |
| 16 | Canberra Institute of Technology: Staff and Student Records audit | August 2004 | Yes |

[1227] OAIC 'Privacy reports – archive'< http://www.oaic.gov.au/privacy/privacy-archive/privacy-reports-archive/Page-2>

| | | | |
|---|---|---|---|
| 17 | ACT Department of Disability, Housing and Community Services: Client Records audit | August 2005 | Yes |
| 18 | Department of Foreign Affairs and Trade & Australian Customs Service: ePassport & SmartGate Trials audit | October 2005 | Yes |
| 19 | ACT Department of Justice And Community Safety: Registrar General's Office audit | October 2005 | Yes |
| 20 | ACT Office of the Community Advocate (now ACT Public Advocate): Client Records audit | July 2006 | Yes |
| 21 | ACT Corrective Services: Client and Staff Records audit | November 2006 | Yes |
| 22 | Australian Customs Service: SmartGate Automated Border Processing audit | April 2007 | Yes |
| 23 | Department of Foreign Affairs and Trade, Department of Immigration and Multicultural Affairs and Centrelink: Document Verification Service Prototype audit | May 2007 | Yes |
| 24 | ACT Planning and Land Authority audit | May 2008 | Yes |
| 25 | Public Trustee for the Australian Capital Territory audit | May 2009 | Yes |
| 26 | Passenger Name Records (PNR data) Audit Report No 1 | December 2009 | Yes |
| 27 | Passenger Name Records (PNR data) Audit Report No 2 | January 2010 | Yes |

## Appendix L
## FOI Request

-----Original Message-----
From: Jean Siganto
Sent: Tuesday, 21 May 2013 9:15 PM
To: foi@oaic.gov.au
Subject: Office of Australian Information Commissioner Own Motion Investigations – Freedom of Information Request

I request access to documents of the Office of Australian Information Commissioner (OAIC) relating to the following Own Motion Investigations conducted by the Privacy Commissioner:

- Vodafone Hutchison Australia (February 2011)
- Sony PlayStation Network / Qriocity (September 2011)
- Telstra Corporation Limited (June 2012)
- Dell Australia/Epsilon (June 2012)
- Medvet Science Pty Ltd (July 2012)

The documents I would like to be disclosed are all those held by OAIC which relate in any way to the above investigations including:

- All documents relating to the making of the decision by the OAIC to launch own motion investigations in each of the cases

- All documents relating to the development, finalisation and implementation of an investigation plan or other methodology for the conduct of each of the investigations

- All correspondence between the OAIC and the parties being investigated and any third parties relating to or forming part of the investigations, including correspondence from the OAIC advising that an investigation may be or has been commenced and requesting that information be provided

- All documents relevant to the assessment by the OAIC of whether or not there had been any breach of the *Privacy Act* 1988 (Cth) as part of any of the investigations

- All documents relevant to the Privacy Commissioner's decision-making process and the making of the final decision in each case, including any internal memorandum or other briefing papers

- All documents relevant to any on-going communications between the OAIC and any investigated party relevant to the

investigations including, for example, documents relating to the OAIC decision to publish a report of the investigation or the communication by an investigated party to the OAIC on any follow up activities taken by them.

Please note that my interest is largely in regard to the operational workings of the OAIC in the conduct of own motion investigations. In particular:

- I am not interested in obtaining the personal details or other identifying information of any of the third parties (including any of their staff or officers) involved in any of these investigations. I am happy for all personal details and any other identifying information relating to those third parties to be redacted.

- I am also not interested in receiving any confidential information provided to you such as, for example, the security measures that were in place at the time of the incident. I am happy for this information to be redacted from the documents to be provided.

I note that access to this information will support the objects of the Freedom of Information Act 1982 (Cth) including:

- increasing public participation in Government processes, with a view to promoting better-informed decision-making; and

- increasing scrutiny, discussion, comment and review of the Government's activities.

In addition, I believe that it would be in the public interest (for the purposes of Section 11A(5) of the FOI Act) to disclose any documents that might otherwise be conditionally exempt, as disclosure would:

- Enhance the accountability and scrutiny of government decision-making;

- Provide context and background to the operations of the OAIC and the OAIC’s investigation process; and

- Inform debate on a matter of public importance

My contact details are as follows:

Contact Phone: (07) 3138 2166 or Mobile: 0408 275 733 Contact Email: jj.siganto@student.qut.edu.au

Address:

Ms J Siganto

Faculty of Law

Queensland University of Technology

GPO Box 2434

Brisbane QLD 4001

Please let me know if I can provide any further information about or clarification of my request.

I look forward to hearing from you in due course.

Best regards,

Jodie Siganto

## Appendix M
## OAIC Guidance

### Guidelines as at 10 September 2014[1228]

| | Name of Guideline | Date Issued/Last Updated |
|---|---|---|
| 1 | APP Guidelines | March 2014 |
| 2 | Guidelines on Data Matching in Australian Government Administration | June 2014 |
| 3 | Guidelines for developing codes | September 2013 |
| 4 | Guidelines for recognising external dispute resolution schemes | September 2013 |

### Guides as at 10 September 2014[1229]

| | Name of Guide | Date Issued/Last Updated |
|---|---|---|
| 1 | Mobile privacy: a better practice guide for mobile app developers | September 2014 |
| 2 | TPP quick reference tool (ACT Agency Privacy Principles) | September 2014 |

[1228] OAIC 'APP Guidelines' < http://www.oaic.gov.au/privacy/applying-privacy-law/app-guidelines/>, OAIC 'Advisory Privacy Guidelines' < http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/>

[1229] OAIC 'Privacy Guides' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/>

| | | |
|---|---|---|
| 3 | Data breach notification — A guide to handling personal information security breaches | August 2014 |
| 4 | Privacy public interest determination guide | June 2014 |
| 5 | Guide to developing an APP privacy policy<br>supported by:<br>What to look for in a privacy policy (1 page Post)<br>Guide to developing an APP privacy policy — summary | May 2014 |
| 6 | Guide to undertaking privacy impact assessments<br>Guide to undertaking privacy impact assessments — summary | May 2014 |
| 7 | Guide to the Privacy (Persons Reported as Missing) Rule 2014 | March 2014 |
| 8 | APP quick reference tool | March 2014 |
| 9 | Australian Privacy Principles and National Privacy Principles – Comparison Guide | April 2013 |
| 10 | Guide to information security — April 2013 | April 2013 |
| 11 | NPPs - Plain English Summary | Undated |
| 12 | IPPs - Plain English Summary | Undated |
| 13 | Automated Assistance in Administrative Decision-Making - Better Practice Guide (Non-OPC document with OPC contributions) (February 2007) | August 2007 |
| 14 | Guidelines for Federal and ACT Government Websites | March 2003 |

| | | |
|---|---|---|
| 15 | Privacy and Public Key Infrastructure: for Agencies using PKI to communicate or transact with individuals | December 2001 |
| 16 | Privacy in the Private Health Sector | November 2001 |
| 17 | Guidelines to the National Privacy Principles | September 2001 |
| 18 | Guidelines to Information Privacy Principles 4 - 7 | February 1998 |
| 19 | Guidelines to Information Privacy Principles 8 - 11 | November 1996 |
| 20 | Guidelines to Information Privacy Principles 1 - 3 | October 1994 |
| 21 | Covert surveillance in Commonwealth administration guidelines | |

**Privacy fact sheets as at 10 September 2014**[1230]

| | Name of fact sheet | Date Issued/Last Updated |
|---|---|---|
| 1 | Privacy fact sheet 42: Australian Capital Territory Privacy Principles | September 2014 |
| 2 | Privacy fact sheet 41: Commonwealth spent convictions scheme:<br>• Long text description for the Commonwealth spent convictions scheme: A step-by-step guide flow chart | May 2014 |
| 3 | Privacy fact sheet 40: Credit providers, the APPs and your credit report | May 2014 |
| 4 | Privacy fact sheet 39: Direct marketing and your credit report | May 2014 |
| 5 | Privacy fact sheet 38: Hardship assistance and your credit report | May 2014 |
| 6 | Privacy fact sheet 37: Fraud and your credit report | May 2014 |
| 7 | Privacy fact sheet 36: When will the information on your credit report be deleted | May 2014 |
| 8 | Privacy fact sheet 35: When can a default be included in your credit report | May 2014 |

[1230] OAIC 'Privacy Fact Sheets' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/>

| | | |
|---|---|---|
| 9 | Privacy fact sheet 34: Repayment history information and your credit report | May 2014 |
| 10 | Privacy fact sheet 33: Making a credit reporting complaint | May 2014 |
| 11 | Privacy fact sheet 32: Seeking correction of your credit report | May 2014 |
| 12 | Privacy fact sheet 31: How you can access your credit report | May 2014 |
| 13 | Privacy fact sheet 30: How the personal information in your credit report can be used | May 2014 |
| 14 | Privacy fact sheet 29: Who can access your credit report | May 2014 |
| 15 | Privacy fact sheet 28: What information can be included in your credit report | May 2014 |
| 16 | Privacy fact sheet 27: Credit reporting series glossary | May 2014 |
| 17 | Privacy fact sheet 26: Credit reporting series contents and overview | May 2014 |
| 18 | Privacy fact sheet 25: Credit reporting in Australia – summary | May 2014 |
| 19 | Privacy fact sheet 24: How changes to privacy law affect you | May 2014 |
| 20 | Privacy fact sheet 23: Emergency access and your eHealth record | Updated September 2014 |
| 21 | Privacy fact sheet 22: Medicare and your eHealth record | Updated September |

| | | |
|---|---|---|
| | | 2014 |
| 22 | Privacy fact sheet 21: Young people and the eHealth record system | Updated September 2014 |
| 23 | Privacy fact sheet 20: Consent and the handling of personal information in your eHealth record | Updated September 2014 |
| 24 | Privacy fact Sheet 19: How to manage your eHealth record | Updated September 2014 |
| 25 | Privacy fact sheet 18: The OAIC and the eHealth record system | Updated September 2014 |
| 26 | Privacy fact sheet 17: Australian Privacy Principles | February 2013 (amended January 2014) |
| 27 | Privacy fact sheet 15: Ten tips for protecting the personal information in your eHealth record | Updated September 2014 |
| 28 | Privacy fact sheet 12: Conciliation of privacy complaints | June 2012 |
| 29 | Privacy fact sheet 11: How will the OAIC handle a privacy complaint against my organisation? | June 2012 |
| 30 | Privacy fact sheet 10: What will happen to my complaint? | June 2012 |
| 31 | Privacy fact sheet 9: Guide to internal investigations | April 2012 |
| 32 | Privacy fact sheet 8: Ten steps to protect your personal information | April 2012 |

| | | |
|---|---|---|
| 33 | Privacy fact sheet 7: Ten steps to protect other people's personal information | April 2012 |
| 34 | Privacy fact sheet 6: The binding Tax File Number Guidelines 2011 and the protection of tax file number information | Updated March 2102 |
| 35 | Privacy fact sheet 5: Digital photocopiers: inadvertent collection and storage of personal information | December 2011 |
| 36 | Privacy fact sheet 4: Online behavioural advertising — know your options | June 2011 |
| 37 | Privacy fact sheet 3: 4A framework — A tool for assessing and implementing new law enforcement and national security powers | July 2011 |
| 38 | Privacy fact sheet 2: National Privacy Principles | July 2011 |
| 39 | Privacy fact sheet 1: Information Privacy Principles under the *Privacy Act* 1988 | July 2011 |
| 40 | My Privacy My Choice | Undated |
| 41 | My Health My Privacy My Choice - a consumer's guide to privacy and health information (November 2002) | November 2002 |
| 42 | Information Sheet (Public and Private Sectors) 1 - Emergencies and disasters | April 2010 |
| 43 | Information Sheet (Private Sector) 7 - 2001: Unlawful Activity and Law Enforcement | December 2001 |
| 44 | Information Sheet (Private Sector) 5 - 2001: Access and the Use of Intermediaries | December 2001 |
| 45 | Information Sheet (Private Sector) 4 - 2001: Access | May 2009 |

| | | |
|---|---|---|
| | and Correction | |
| 46 | Information Sheet (Private Sector) 30 - 2010: ID scanning in clubs and pubs | April 2010 |
| 47 | Information Sheet (Private Sector) 3 - 2001: Openness | December 2001 |
| 48 | Information Sheet (Private Sector) 29 - 2009: Use or disclosure of genetic information in the private health sector | December 2009 |
| 49 | Information Sheet (Private Sector) 28 - 2009: NPP 3 Data Quality | May 2009 |
| 50 | Information Sheet (Private Sector) 26 - 2008: Interaction between the *Privacy Act* and the Spam Act | April 2008 |
| 51 | Information Sheet (Private Sector) 25 - 2008: Sharing health information to provide a health service | March 2008 |
| 52 | Information Sheet (Private Sector) 24 - 2008: Disclosure of health information and impaired capacity | March 2008 |
| 53 | Information Sheet (Private Sector) 23 - 2008: Use and disclosure of health information for management, funding and monitoring of a health service | March 2008 |
| 54 | Information Sheet (Private Sector) 22 - 2008: Fees for access to health information under the *Privacy Act* | March 2008 |
| 55 | Information Sheet (Private Sector) 21 - 2008: Denial of access to health information due to a serious threat to life or health | March 2008 |
| 56 | Information Sheet (Private Sector) 20 - 2007: | August 2007 |

| | | |
|---|---|---|
| | Scanning "Proof of Identity" Documents | |
| 57 | Information Sheet (Private Sector) 19 - 2007: The Prescription Shopping Information Service (PSIS) and The *Privacy Act* | April 2007 |
| 58 | Information Sheet (Private Sector) 18 - 2003: Taking reasonable steps to make individuals aware that personal information about them is being collected | June 2003 |
| 59 | Information Sheet (Private Sector) 17 - 2003: Privacy and Personal Information that is Publicly Available | February 2003 |
| 60 | Information Sheet (Private Sector) 16 - 2002: Application of Key NPPs to Due Diligence and Completion when Buying and Selling a Business | October 2002 |
| 61 | Information Sheet (Private Sector) 15 - 2002: National Privacy Principle 7 - Identifiers in the Health Sector | April 2002 |
| 62 | Information Sheet (Private Sector) 14 - 2001: Privacy Obligations for Commonwealth Contracts | December 2001 |
| 63 | Information Sheet (Private Sector) 12 - 2001 Coverage of and Exemptions from the Private Sector Provisions | 2001 |

**Privacy Agency Resources as at 10 September 2014**[1231]

[1231] OAIC 'Privacy Agency Resources' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-agency-resources/>

| | Name of Privacy Agency Resource | Date Issued/Last Updated |
|---|---|---|
| 1 | Privacy agency resource 3: Information Privacy Act 2014 — Checklist for ACT agencies | September 2014 |
| 2 | Privacy agency resource 2: Privacy Act reforms – Checklist for APP entities (agencies) | May 2013 |
| 3 | Privacy agency resource 1: Individual healthcare identifiers — Compliance obligations for state and territory healthcare providers | September 2014 |
| 4 | Provision of personal information to members of Parliament | August 1990 |

**Privacy Business Resources as at 10 September 2014**[1232]

| | Name of Privacy Business Resource | Date Issued/Last Updated |
|---|---|---|
| 1 | Privacy business resource 6: Healthcare identifiers and the eHealth record system | September 2014 |
| 2 | Privacy business resource 5: Healthcare Identifiers — General information for healthcare providers | September 2014 |
| 3 | Privacy business resource 4: De-identification of data and information | April 2014 |
| 4 | Privacy business resource 3: Credit reporting — what has changed | June 2013 |

[1232] OAIC 'Privacy Business Resources' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/>

| | | |
|---|---|---|
| 5 | Privacy business resource 2: Privacy Act reforms – Checklist for APP entities (organisations) | May 2013 |
| 6 | Privacy business resource 1: Individual Healthcare Identifiers—Compliance obligations of private healthcare providers | September 2014 |
| 7 | Snapshot of the Privacy Act for Small Business | November 2007 |
| 8 | Privacy Checklist for Small Business | November 2007 |
| 9 | Advice for credit providers and credit reporting agencies when contracting out record management functions | May 1996 |
| 10 | Credit Reporting Advice Summaries (April 2002) | April 2002 |
| 11 | Health Information and the Privacy Act 1988—A Short Guide for the Private Health Sector (January 2002) | January 2002 |
| 12 | Information Sheet (Private Sector) 9—2001: Handling Health Information for Research and Management | December 2001 |
| 13 | Information Sheet (Private Sector) 8 — 2001: Contractors | December 2001 |

# Bibliography

## ARTICLES, BOOKS, REPORTS


Adams, Carolyn, 'One office, three champions? Structural integration in the office of the Australian Information Commissioner' (2014) 21 *A J Admin L*

Administrative Review Council, *Decision-making: Evidence, Facts and Findings* (August 2007) <http://www.arc.ag.gov.au/Publications/Reports/Pages/Downloads/ARCBestPracticeGuide3EvidenceFactsandFindings.aspx> ('*ARC Evidence Guide*').

Administrative Review Council, *Decision-making: Reasons* (August 2007) < http://www.arc.ag.gov.au/Documents/Revised+Best+Practice+Guide+4+-+Reasons+-+24+April+2008.pdf > ('*ARC Decision Guide*').

Alexander, Charles, Elisabeth Koster and Helen Paterson, 'Punitive powers guided by ambiguity: the Australian Federal Privacy Commissioner's new powers in the context of a principles-based privacy regime' (2013) 9(5) *Privacy Law Bulletin* 66

Almond, Carl 'Should vendors be liable for security flaws in software?' (2009) (4) *Computer Fraud & Security* 4

Aquilina, Kevin, 'Public security versus privacy in technology law: A balancing act?' (2010) 26(2) *Computer Law & Security Review* 130

Agresti, W. W., 'The Four Forces Shaping Cybersecurity' 43(2) *Computer* 101

Arnold, Bruce, 'Ending the OAIC and new frameworks for privacy law' (2014) 11(5) *Privacy Law Bulletin* 66

Asia Pacific Economic Co-Operation Secretariat, 'APEC Privacy Framework' (2005) <http://www.ema.gov.au/www/agd/rwpattach.nsf/VAP/%2803995EABC73F94816C2AF4AA2645824B%29~APEC+Privacy+Framework.pdf/$file/APEC+Privacy+Framework.pdf>

Australian Attorney General, *Protective Security Policy Framework Securing Government business* (Attorney General's Department, 2010)

Australian Government, 'The Australian Government Guide to Regulation' (2014) <http://www.cuttingredtape.gov.au/sites/default/files/documents/australian_government_guide_regulation.pdf>

Australian Government *Best Practice Regulation Handbook* (2007)

Australian Government, *First Stage Response to the Australian law Reform Commission Report 108* (Australian Government, October 2009) <http://www.dpmc.gov.au/privacy/alrc_docs/stage1_aus_govt_response.pdf>.

Australian Government Information Management Office, *Commercial Service Provider Assurance Framework* (Department of Finance, September 2012)

Australian Law Reform Commission, *For Your Information: Australian Privacy Law and Practice,* Report No 108 (2008)

Australian Law Reform Commission, *Review of Privacy Issues Paper 31,* (2006) <http://www.alrc.gov.au/ip-31>

Australia Prudential Regulation Authority, *PPG 234 - Management of security risk in information and information technology* (1 February 2010) <http://www.apra.gov.au/CrossIndustry/Documents/PPG_PPG234_MSRIT_012010_v7.pdf> (‘*PPG 234*’).

Australian Signals Directorate, *Top 4 Mitigation Strategies to Protect Your ICT System* (2012) <http://www.dsd.gov.au/publications/csocprotect/Top_4_Mitigations.pdf?&verNov12 >

Australian Signals Directorate, *Australian Government Information Security Manual - Principles* (September 2012)

Australian Signals Directorate, *Australian Government Information Security Manual - Controls* (April 2013)

Axelrod, C Warren, Jennifer Bayuk and Daniel Schutzer (eds), *Enterprise Information Security and Privacy* (Artech House Books, 2009)

Ayres, I and J Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press, 1992)

Backhouse, James, Carol W. Hsu and Leiser Silva, 'Circuits of Power in Creating De Jure Standards: Shaping an International Information Systems Security Standard' (2006) 30 *MIS Quarterly* 413

Baldwin, R *Better Regulation: Is it better for business?* (Federation of Small Business, 2007).

Baldwin, Robert and Julia Black, 'Really Responsive Regulation' (2008) 71(1) *The Modern Law Review* 59

Baldwin, Cave and Lodge, *The Oxford Handbook of Regulation* (Oxford University Press, 2010).

Baldwin, R , M Cave and M Lodge, *Understanding Regulation Theory Strategy and Practice* (Oxford University Press, Second ed, 2012)

Bambauer, Derek K, 'Rules, Standards and Geeks' (2010 - 2011) 5 *Brook. J. Corp. Fin. & Com. L.* 49

Bambauer, Derek E., 'Ghost in the Network' (2014) 162 *University of Pennsylvania Law Review* 1011

Bambauer, Derek E., 'Privacy Versus Security' (2013) 103 (3) *Journal of Criminal Law and Criminology,* 667.

Bamberger, K, 'Technologies of Compliance: Risk and Regulation in the Digital Age' (March 2010) 88(4) *Texas Law Review* 669

Bamberger, K and D Mulligan, 'Privacy on the Books and on the Ground' (2011) 63 Stan. L. Rev. 247

Bamberger, K and D Mulligan, 'New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the United States: An Initial Inquiry' 33(4) *Law & Policy*

Barnard-Wills, David, 'Security, privacy and surveillance in European policy documents' (2013) 3(3) (August 1, 2013) *International Data Privacy Law* 170

Barrett, Pat 'Commentary on Malcolm Crompton's Paper entitled "Light Touch or Soft Touch?: Reflections of a regulatory implementing a new privacy regime"' (Speech delivered at National Institute of Governance, University of Canberra, 18 March 2004).

Barwick, Hamish, 'Data breach liability should lie with companies: Survey' (2012) *Computerworld (*online*)*

Baumer, David L., Julia B. Earp and J. C. Poindexter, 'Internet privacy law: a comparison between the United States and the European Union' (2004) 23(5) *Computers & Security* 400

Bendall, Anthony 'The governance of privacy: speak softly and carry a big stick' (2009) 60 *Australian Institute of Administrative Law National Forum* 39

Bennett, S. C. 'Data Security for Lawyers.' (June 2011) 83(5) *Journal (New York State Bar Association)* 2

Bennett, Colin J and Charles D I Raab, *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2nd revised ed, 2006).

Better Regulation Task Force, *Principles of Good Regulation* (UK Cabinet Office, 2003).

Bidgoli, Hossein (ed), *Global perspectives in information security : legal, social and international issues* (John Wiley & Sons, 2006)

Bishop, Derek A. 'To Serve and Protect: Do Businesses Have a Legal Duty to Protect Collections of Personal Information?' 3 *Shindler Journal of Law, Commerce & Technology* 7

Bishop, Jonathan, 'Tough on data misuse, tough on the causes of data misuse: A review of New Labour's approach to information security and regulating the misuse of digital information (1997–2010)' (2010) 24(3) *International Review of Law, Computers & Technology* 299

Black, Julia, 'Forms and paradoxes of principles-based regulation' (2008) 3(4) *Capital Markets Law Journal* 425

Black, Julia, 'Managing Regulatory Risks and Defining the Parameters of Blame: A Focus on the Australian Prudential Regulation Authority' (2006) 28(1) *Law & Policy* 1

Black, Julia, *Principles Based Regulation: Risks, Challenges and Opportunities* (London School of Economics and Political Science, 2007)

Black, Julia, 'When risk-based regulation aims low: Approaches and challenges' (2012) 6 *Regulation & Governance* 18

Black, J., 'The Rise, Fall and Fate of Principles Based Regulation' (Working Paper no 17, London School of Economics and Political Science, 2010)

Black, Julia and Robert Baldwin, 'Really Responsive Risk-Based Regulation' (2010) 32(2) *Law & Policy* 181

Black, J. and Robert Baldwin, 'When risk-based regulation aims low: A strategic framework' (2012) 6(2) *Regulation & Governance* 131

Blank, Andrew G., *TCP/IP Foundations* (Sybex, Alameda, USA, 2004)

Bloom, Geoff and Kristina Frketic, 'The OAIC's new Guide to Information Security, the hacking of 77 million Sony users, and the privacy breach that cost $171 million' (2013) 9(9) *Privacy Law Bulletin* 150.

Bodin, Lawrence D., Lawrence A. Gordon and Martin P. Loeb, 'Information Security and Risk Management' (2008) 51(4) *Communications of the ACM* 64

Boehmer, W., 'Appraisal of the Effectiveness and Efficiency of an Information Security Management System Based on ISO 27001' (Paper presented at the Emerging Security Information, Systems and Technologies, 2008. 25-31 August 2008)

Bojanc, Rok, Borka Jerman-Blažič and Metka Tekavčič, 'Managing the investment in information security technology by use of a quantitative modeling' (48) 6 *Information Processing & Management* 1031.

Bradshaw, Simon, Christopher Millard and Ian Walden, 'Contracts for clouds: comparison and analysis of the Terms and Conditions of cloud computing services' (2011) 19(3) (September 21, 2011) *International Journal of Law and Information Technology* 187

Braithwaite, J, *Restorative Justice and Responsive Regulation* (Oxford University Press, 2002)

Breaux, Travis D. and David L. Baumer, 'Legally "reasonable" security requirements: A 10-year FTC retrospective' (2011) 30(4) *Computers & Security* 178

Broderick, J. Stuart, 'ISMS, security standards and security regulations' (2006) 11(1) *Information Security Technical Report* 26

Brownsword, R.R., 'The Challenge of Regulatory Effectiveness' *Rights, Regulation, and the Technological Revolution* (Oxford University Press, 2008)

Burdon, Mark, 'Contextualizing the Tensions and Weaknesses of Information Privacy and Data Breach Notification Laws' (2010 - 2011) 27 *Santa Clara Computer & High Tech. L.J.* 63

Burdon, Mark, Jason Reid and Rouhshi Low, 'Encryption safe harbours and data breach notification laws' (2010) 26(5) *Computer Law & Security Review* 520

Burdon, Mark and Paul Telford, 'The Conceptual Basis of Personal Information in Australian Privacy Law' (2010) 17(1) *Murdoch University Electronic Journal of Law* 27

Burdon, Mark et al, 'Stakeholder Perspectives Regarding the Mandatory Notification of Australian Data Breaches' (2009) 15 (2) *Media and Arts Law Review* 149

Burdon, Mark and Alissa McKillop, 'The Google Street View Wi-Fi Scandal and its Repercussions for Privacy Regulation' (2014) 39(3) *Monash University Law Review* 702

Burstein, Aaron J., 'How a Framework for Information Security Law Could Improve Information Security' (2008)

Bygrave, Lee *Data Protection Law: Approaching its Rationale, Logic and Limits* (Kluwer, 2002)

Bygrave, Lee A 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law - Part 1' (2000) 7(1) *Privacy Law and Policy Reporter* 11

Bygrave, Lee A, 'Where have all the judges gone? Reflections on judicial involvement in developing data protection law - Part 2' (2000) 7(2) *Privacy Law and Policy Reporter* 3

Bygrave, Lee A. and Jon Bing (eds), *Internet Governance: Infrastructure and Institutions* (Oxford University Press, 2009)

Camp, L. Jean, 'The State of Economics of Information Security' (2006) 2 *I/S:A Journal of Law and Policy for the Information Society* 10

Cassini, J., B. D. Medlin and A. Romaniello, 'Forty Years of Federal Legislation in the Area of Data Protection and Information Security' in H. (Ed.)

Nemati (ed), *Pervasive Information Security and Privacy Developments: Trends and Advancements* (IGI Global, 2011) 14

Cate, F.H., 'Information Security Breaches: Looking Back and Thinking Ahead (2008)' (2008) <http://www.hunton.com/files/tbl_s47Details/FileUpload265/2308/Information_Security_Breaches_Cate.pdf>

Cave, Martin, *The Oxford handbook of regulation* (Oxford University Press. , 12/08/2010)

Cavoukian, Ann and Mark Chanliaj, 'Privacy and Security by Design: A convergence of paradigms' (Information and Privacy Commissioner, Canada, 2013) <http://www.privacybydesign.ca/content/uploads/2013/01/pbd-convergenceofparadigms.pdf>

Cavoukian, Ann, 'Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era' in *Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards* (IGI Global, 2012)

Centre for Freedom of Information, *Commissioners Report Low Budgets, Growing Workloads* (12 April 2013) <http://www.freedominfo.org/2013/04/commissioners-report-low-budgets-growing-workloads>

Chandler, Jennifer, 'Information Security, Contract and Liability' (2010) 84 *Chicago-Kent Law Review*

Charlesworth, Andrew, 'The future of UK data protection regulation' (2006) 11(1) *Information Security Technical Report* 46

Citron, Danielle Keats, 'Reservoirs of Danger: The Evolution of Public and Private Law at the Dawn of the Information Age' (January 2007) 80 *S. Cal. L. Rev.*

Clark, Eugene, *Cyberlaw in Australia* (Kluwer, 2010)

Clarke, Roger, *Challenges Facing the OECD's Revised Security Guidelines* (2013) <http://www.rogerclarke.com/SOS/OECDS-1311.html>.

Cohen, Fred, ‘On the implications of computer viruses and methods of defense’ (1988) 7(2) *Computers & Security Journal* 167

Coles-Kemp, Lizzie, 'Information security management: An entangled research challenge' (2009) 14(4) *Information Security Technical Report* 181

Commonwealth Ombudsman, ‘Better Practice Guide to Complaint Handling’, (April 2009) < http://www.ombudsman.gov.au/docs/better-practice-guides/onlineBetterPracticeGuide.pdf>

Commonwealth of Australia, House of Representatives, Parliamentary Debates, 8 November 2000 at 22370 (D Williams-Attorney-General).

Conradi, Mike, 'Legal developments in IT security' (2007) 23(4) *Computer Law & Security Review* 365

Correiae, R., L. Pirmez and L. F. R. C. Carmo, 'Evaluating Security Risks following a Compliance Perspective' (Paper presented at the High Assurance Systems Engineering Symposium, 2008. HASE 2008. 11th IEEE, 3-5 Dec. 2008 2008)

Crompton, Malcolm 'Are Comparisons Possible? A framework for assessing the performance of data protection supervisors' (Paper presented at 27th International Conference of Data Protection and Privacy Commissioners, Montreux, Switzerland, 15 September 2005) <http://www.iispartners.com/Publications/index.html#reg>

Crompton, Malcolm 'Light Touch or Soft Touch?: Reflections of a regulatory implementing a new privacy regime' (Speech delivered at National Institute of Governance, University of Canberra, 18 March 2004).

Cronin, Kevin, 'Best Practices and the State of Information Security' (2009-2010) 84 *Chicago-Kent Law Review* 811

Crossler, Robert E. et al, 'Future directions for behavioral information security research' (2013) 32(0) *Computers & Security* 90

Crowe, J, 'The Role of contextual meaning in judicial interpretation' (2013) 41 *Federal Law Review* 417

Culnan, Mary J., 'Accountability as the Basis for Regulating Privacy: Can Information Security Regulations Inform Privacy Policy?' (Bentley University, July 20, 2011) <http://www.futureofprivacy.org/wp-content/uploads/2011/07/Accountability%20as%20the%20Basis%20for%20Regulating%20Privacy%20Can%20Information%20Security%20Regulations%20Inform%20Privacy%20Policy.pdf>

Curtin, Matthew C and Lee T. Ayres, 'Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry' (2009) *Interhack* 47 <http://web.interhack.com/publications/breach-taxonomy>

Cyra, Lukasz and Janusz Gorski, 'SCF — A framework supporting achieving and assessing conformity with standards' (2011) 33(1) *Computer Standards & Interfaces* 80

Da Veiga, A. and J. H. P. Eloff, 'A framework and assessment instrument for information security culture' (2010) 29(2) *Computers & Security* 196

Davies, Simon, 'Unprincipled Privacy: Why the Foundations of Data Protection Are Failing Us' (2001) 24 *U.N.S.W.L.J.* 284

De Villiers, Meiring, 'Information Security Standards and Liability' (2010) 13 *Journal of Internet Law* 24

De Villiers, Meiring, 'Reasonable Foreseeability in Information Security Law: A Forensic Analysis' (2008) *Hastings Coom/Ent L. J.* 100

DeKay, Sam and Ken Belva, 'Privacy Roles and Responsibilities' in *Enterprise Information Security and Privacy* (2009)

Deloitte, *Ministry of Social Development - Independent Review of Information Systems Security* (November 2012) <http://www.msd.govt.nz/documents/about-msd-and-our-work/newsroom/media-releases/2012/independent-review-deloitte.pdf>

DeNardis, Laura 'A History of Internet Security'in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007)

Denning,P. J., *Computers under attack: intruders, worms, and viruses* (Addison-Wesley Publishing Company, United States of America, 1991)

Department of the Prime Minister and Cabinet, 'Issues Paper A Commonwealth Statutory Cause of Action for Serious Invasion of Privacy' (2011) <http://www.dpmc.gov.au/privacy/causeofaction/>

Deverich, Carolyn A., Brian R. Strange, David A. Holop, 'Into the Breach' (February, 2012) *Los Angeles Lawyer*

Dieckmann, John, 'The new APP 8: crack down on cross-board data flows' (2012) 8(10) *Privacy Law Bulletin* 270

Diffie, Whitfield, 'Information Security: 50 years Behind, 50 Years Ahead' (2008) 51(1) *Association for Computing Machinery. Communications of the ACM* 55

Dixon, Tim (ed), *Australian privacy reporter: a guide to privacy law and practice* (2014).

Dlamini, M. T., J. H. P. Eloff and M. M. Eloff, 'Information security: The moving target' (2009) 28(3–4) *Computers & Security* 189

Douglas-Stewart, Jeremy, *Annotated National Privacy Principles* (Presidian, 2009)

Dourish, P. and K. Anderson, 'Collective information practice: exploring privacy and security as social and cultural phenomena.' (2006) 21(3) *Human-computer interaction* 319

Doyle, Carolyn and Mirko Bagaric, *Privacy Law in Australia* (The Federation Press, 2005)

Edward, Humphreys, 'Information security management standards: Compliance, governance and risk management' (2008) 13(4) *Information Security Technical Report* 247

Epstein, Richard A and Thomas P Brown, 'Cybersecurity in the Payment Card Industry' (2008) 75 *University of Chicago Law Review* 203

Everett, Cath, 'Is ISO 27001 worth it?' 2011 (1) *Computer Fraud & Security* 5

Everett, Cath, 'PCI DSS: Lack of direction or lack of commitment?' (2009) 2009(12) *Computer Fraud & Security* 18

Fels, Allan 'The Role of The Privacy Regulator in an Era of Transparency' Presentation to the 25th International Conference of Data Protection and Privacy Commissioners, September 2003

Feiler, Lukas, *Information Security Law in the EU and the U.S.: A Risk-Based Assessment of Implicit and Explicit Regulatory Policies* (A Joint Initiative of Stanford Law School and the University of Vienna School of Law., 2011) <http://www.law.stanford.edu/program/centers/ttlf/papers/feiler_wp9.pdf>

Financial Services Authority U.K., *Principles Based Regulation: Focusing on the Outcomes that Matter* (2007)

Ford, Cristie L., 'New Governance, Compliance, and Principles-Based Securities Regulation' (2008) 45(1) *American Business Law Journal* 1

Ford, Cristie, 'New Governance in the Teeth of Human Frailty: Lessons from Financial Regulation' (2010) *Wisconsin Law Review* 591

Ford, Cristie and Mary Condon, 'Introduction to "New Governance and the Business Organization" Special Issue of Law and Policy' (2011) 33(4) *Law & Policy* 449

Frankland, Jane, 'IT security metrics: implementation and standards compliance' (2008) 2008(6) *Network Security* 6

Frei, Stefan et al, 'Modelling the Security Ecosystem - The Dynamics of (In)Security' (Paper presented at 8th Annual Workshop on Economics and Information Security, 2009)

Friedman, Allan, 'Economic and Policy Frameworks for Cybersecurity Risks' (2011)

Freiberg, Arie, *The Tools of Regulation* (The Federation Press, 2010)

Georgia Institute of Technology "Emerging Cyber Threats Report 2013" <http://www.gtsecuritysummit.com/pdf/2013ThreatsReport.pdf> Last accessed December 17, 2012

Gilad, Sharon, 'It runs in the family: Meta-regulation and its siblings' (2010) 4(4) *Regulation & Governance* 485

Gilad, Sharon, 'Beyond Endogeneity: How Firms and Regulators Co-Construct the Meaning of Regulation' (2014) 36(2) *Law & Policy* 134

Gatzlaff, Kevin M. and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth' (2010) 13(1) *Risk Management and Insurance Review* 61

Genetski, Christian S., 'Liability from Security Breaches and Other Disclosures of Personal Information: A Growing Trend' (Paper presented to the Practising Law Institute, March 2007)

Gifford, Nick, *Information security: managing the legal risks* (CCH Australia Limited, 2009)

Gikas, Constantine 'A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards' (2010) 19(3) *Information Security Journal: A Global Perspective* 9

Gilad, Sharon, 'It runs in the family: Meta-regulation and its siblings' (2010) 4(4) *Regulation & Governance* 485

Gillies, Alan, 'Improving the quality of information security management systems with ISO 27000' (2011) 23(4) *The TQM Journal* 367

Goldberg, Alan, 'When Are Reasons for Decision Considered Inadequate?' (2000) 2 *AIAdminLawF* 1

Goodman, Seymour E. and Herbert S. Lin, 'Toward a Safer and More Secure Cyberspace' (2007)

Gotlieb, Calvin C., 'Privacy: A Concept Whose Time Has Come and Gone' in D. Lyon and E. Zureik (eds), *Surveillance, Computers and Privacy* (University of Minnesota Press, 1995)

Greenleaf, Graham, 'An Endnote on Regulating Cyberspace: Architecture vs Law?' (1998) 21(2) *University of New South Wales Law Journal* 593

Graham Greenleaf, 'The "Tabula Rasa": Ten Reasons Why Australian Privacy Law Does Not Exist' (2001) 24(1) University of New South Wales Law Journal 262

Greenleaf, Graham, 'APEC's Privacy Framework: A new low standard' (2005) 11(5) *Privacy Law & Policy Reporter* 1

Greenleaf, Graham, 'Reforming reporting of privacy cases: A proposal for improving accountability of Asia-Pacific Privacy Commissioners' in Paul Roth (ed), *Privacy Law And Policy In New Zealand* (Butterworths LexisNexis, 2003)

Greenleaf, Graham, 'Five Years of the APEC Privacy Framework: Failure or promise?' (2009) 25(1) *Computer Law & Security Report* 28

Greenleaf, Graham, 'The Influence of European Data Privacy Standards outside Europe: Implications for globalization of Convention 108' (2012) 2(2) *International Data Privacy Law* 68

Greenleaf, Graham, 'Global Data Privacy Laws: 89 Countries, and Accelerating' (2012) *Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012*

Greenleaf, Graham 'Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories' (2013) 23(1) *Journal of Law, Information & Science* 4

Graham Greenleaf and Nigel Waters, 'Australia's Privacy Bill 2012: Weaker Principles, Stronger Enforcement' (2012) 118 *Privacy Laws & Business International Report, Issue 115, Special Supplement, February 2012* 16

Graham Greenleaf and Nigel Waters, '"Making privacy law safe for business": Australia's 2012 privacy Bill' (2012) 8(10) *Privacy Law Bulletin* 266.

Graham Greenleaf, Nigel Waters and Lee Bygrave, Submission to the Australian Law Reform Commission *Review of Privacy Issues Paper No 31* (January 2007).

Greenleaf, Graham, Nigel Waters and Lee Bygrave, 'Promoting and Enforcing Privacy Principles: An analysis of ALRC proposals for the role of the Privacy Commissioner,' Submission to the Australian Law Reform Commission, *Review of Australian Privacy Laws Discussion Paper No 72,* December 2007 <http://www.cyberlawcentre.org/ipp/publications/papers/ALRC_DP72_Enforce_final.pdf>

Greer, Damon, 'Safe Harbor—a framework that works' (2011) 1(3) (August 1, 2011) *International Data Privacy Law* 143

Groves, Matthew 'Duty to Inquire in Tribunal Proceedings' (2011) 33 *Sydney Law Review* 177

Gunasekara, Gehan, 'Paddling in unison or just paddling? International trends in reforming information privacy law' (2014) 22(2) *International Journal of Law and Information Technology* 141

Gutwirth, Serge, Yves Poullet and Paul De Hert (eds), *Data Protection in a Profiled World* (Springer, 2010)

Haines, Fiona, 'Addressing the risk, reading the landscape: The role of agency in regulation' (2011) 5(1) *Regulation & Governance* 118

Haines, Fiona, *The Paradox of Regulation: What Regulation Can Achieve and What it Cannot* (Edward Elgar Publishing Limited, 2011)

Haines, Fiona T and Nick Taylor, *The Paradox of Regulation: What Regulation Can Achieve and What it Cannot* (Edward Elgar, 2011)

Harvey, Dean William and Amy White, 'The Impact of Computer Security Regulation on American Companies' (2002) 8 *Texas Wesleyan Law Review* 505.

Hawke, Alan 'Review of the Freedom of Information Act 1982 and Australian Information Commissioner Act 2010' (Australian Government, 2014) <http://www.ag.gov.au/Consultations/Pages/ReviewofFOIlaws.aspx>

Haws, John, '2013 an epic year for data breaches with over 800 million records lost' (2014) *NakedSecurity (Online)* <http://nakedsecurity.sophos.com/2014/02/19/2013-an-epic-year-for-data-breaches-with-over-800-million-records-lost/>

Head, Michael, *Administrative Law Context and Critique* (The Federation Press, 3rd ed, 2012)

Henry J L et al, 'FTC Proposes Broad New Privacy Framework, and Asks "How It Might Apply in the Real World"' (21 December 2010) *K & L Gates* < http://www.klgates.com/ftc-proposes-broad-new-privacy-framework-and-asks-how-it-might-apply-in-the-real-world-12-21-2010/>

Hiller, Janine S. Hiller and David L. Baumer, 'Due Diligence on the Run: Business Lessoms Derived from FTC Actoins to Enforce Core Security Principles' (2009) 45 *Idaho Law Review* 35

Hon, W. Kuan, Christopher Millard and Ian Walden, 'The problem of 'personal data' in cloud computing: what information is regulated?—the cloud of unknowing' (2011) 1(4) (November 1, 2011) *International Data Privacy Law* 211

Hoo, S., 'How much is enough? A risk-management approach to computer security' (Stanford University, CA, 2000) <http://iis-db.stanford.edu/pubs/11900/soohoo.pdf>

Hoofnagle, Chris, 'B.1 - United States of America' (European Commission, 2010)

Horton, Jonathan, 'Towards a real right of privacy [online]' (2003) 29(2) *Monash University Law Review* 8

Hosein, Gus, 'Returning to a Principled Basis for Data Protection' 84 *CHIKLR* 5

Howard, Philip and Kris Erickson, 'Data Collection and Leakage' (2010) 84 *Chicago-Kent Law Review* 8

Hsu, Carol W., 'Frame misalignment: interpreting the implementation of information systems security certification in an organization' (2009) 18(2) *European Journal of Information Systems* 140

Hughes, Gordon, *Data Protection in Australia* (The Law Book Company Limited, 1991)

Hummerston, Mark 'Sword or Shield: The Role of a Regulator' (Paper presented at Interpreting Privacy Principles Symposium, University of New South Wales, 3 June 2007) <http://www.cyberlawcentre.org/ipp/events/symposium07/Sword%20or%20shield.pdf>

Humphreys, Edward, 'Information security management system standards' (2011) 35(1) *Datenschutz und Datensicherheit - DuD* 7

Imwinkelried, Edward J. and Michael Cherry, 'Redress for Loss of Private e-Data' (2009) 45 *JTLATRIAL* 48

Information Commissioner's Office, *Data Protection Regulatory Action Policy Version 2.0* (UK Government, 2013) <http://ico.org.uk/~/media/documents/library/Data_Protection/Detailed_specialist_guides/data-protection-regulatory-action-policy.pdf>

Information Systems Audit and Control Association, *CISA Review Manual 2006*, (ISACA 2006).

Jackson, Margaret, *Hughes on Data Protection in Australia* (Lawbook Co, 2nd ed, 2001)

Jackson, Margaret and Marita Shelly, *Electronic Information and the Law* (Lawbook Co, 2012)

Jay, Rosemary *Data Protection Law and Practice* (Sweet & Maxwell, 4th ed, 2012)

Jaeger, Paul T., Charles R. McClure and Bruce T. Fraser, 'The structures of centralized governmental privacy protection: approaches, models, and analysis' (2002) 19(3) *Government Information Quarterly* 317

Julisch, Klaus et al, 'Compliance by design - Bridging the chasm between auditors and IT architects' 30(6-7) *Computers & Security* 410

Kemp, Richard, Paul Hinton and Paul Garland, 'Legal rights in data' (2011) 27(2) *Computer Law & Security Review* 139

Kenneally, Erin and John Stanley, 'Beyond Whiffle-Ball Bats: Addressing Identity Crime in an Information Economy' (2008) 26 *Marshall J. Computer & Info. L.* 47

Kennedy, John B., 'National Information Insecurity: Recent Initiatives in Private Sector Information Security' (2010) 20 *Alb. L.J. Sci. & Tech* 385

Kennedy, J. B. , 'Information Security Law Update 2009: The Patchwork Quilt of Regulations Continues to Grow ' (2009) (Tenth Annual Institute on Privacy and Data Security Law) *Practising Law Institute Patents, Copyrights, Trademarks, and Literary Property Course Handbook Series 969*

Kennedy, John B. and Nathan Dee, 'Slouching Towards Federal Data Security Standards for the Private Sector' (2010) 3(10) *Bloomberg Law Reports - Privacy & Information*

Kennedy, J.B. and A.E. Kennedy, 'What Went Wrong? What Went Right? Corporate Responses to Privacy and Security Breaches ' (2007) *Eighth Annual Institute on Privacy and Security Law, Practising Law Institute*

Justice Kirby, Michael 'The history, achievement and future of the 1980 OECD guidelines on privacy' (2011) 1(1) *International Data Privacy Law* 6

KPMG and Information Integrity Solutions, *Independent Review of ACC's Privacy and Security of Information* (August 2012) <http://www.iispartners.com/downloads/22-August-2012-ACC-Independent-Review-FINAL-REPORT.pdf>

Korff, D, 'Thematic Legal Study on assessment of data protection measures and relevant institutions [United Kingdom]' (2009)

Kraemer, Sara, Pascale Carayon and John Clem, 'Human and organizational factors in computer and information security: Pathways to vulnerabilities' (2009) 28(7) *Computers & Security* 509

Krauss, M and H Tipton, *Handbook of Information Security Management* (CRC Press, Boca Raton, Florida, 2012

Kuner, Christopher, 'An international legal framework for data protection: Issues and prospects.' 25(4) *Computer Law & Security Review* 10

Kuner, Christopher et al, 'Privacy—an elusive concept' (2011) 1(3) (August 1, 2011) *International Data Privacy Law* 141

Lacey, David 'Security: Best practice or ancient ritual?' *ComputerWorld UK* (online), 12 January 2011<http://www.computerworlduk.com/in-depth/security/3256436/security-best-practice-or-ancient-ritual/#>.

Langenderfer, Jeff and Don Lloyd Cook, 'Oh, what a tangled web we weave: The state of privacy protection in the information economy and recommendations for governance' (2004) 57(7) *Journal of Business Research* 734

Lapan, Stephen D., Mary-Lynn T. Quartaroli and France J. Reimer, *Qualitative Research: An Introduction* (Wiley, 2001)

Law Reform Commission, *Privacy (1976 - 1983),* Report No 22 (1983) <http://www.alrc.gov.au/sites/default/files/pdfs/publications/alrc22_summary.pdf>.

Law Reform Commission, 'Report 12: Privacy and the Census' (1979) <http://www.alrc.gov.au/inquiries/privacy-1976-83>

Leeuw, Karl de, Maria Michael and Jan Bergestra (eds), *A History of Computer Security Standards*, The History of Information Security: A Comprehensive Handbook (Elsevier, 2007)

Liginlal, Divakaran et al, 'HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory' (2012) 31(2) *Computers & Security* 206

Low, Rouhshi, Mark Burdon and Paul von Nessen, 'Notification of data breaches under the continuous disclosure regime' (2010) 25(2) *Australian Journal of Corporate Law* 70

Ma, Qingxiong, Allen C Johnston and J Michael Pearson, 'Information Security Managegement Objectives and Practices: A Parsimonous Framework' (2008) 16(3) Information Management & Computer Security 251

McConnell, Bruce, 'How to Make Security and Privacy Fit Together' (2008) *Forbes* <http://www.forbes.com/2008/05/14/government-security-privacy-tech-security08-cx_ag_0514private_print.html>

McMillan, John Australian Information Commissioner, and Timothy Pilgrim, Privacy Commissioner, 'The OAIC's enforcement approach to new privacy laws from 12 March 2014' (Statement from the Australian Information Commissioner and Privacy Commissioner, 28 February 2014), < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/oaic-enforcement-approach-to-new-privacy-laws-12-march-2014/the-oaic-s-enforcement-approach-to-new-privacy-laws-from-12-march-2014-statement-from-the-aust>.

Mandelkern Group on Better Regulation *Report on Better Regulation, Final Report* (European Commission, 13 November 2002) <http://ec.europa.eu/smart-regulation/better_regulation/documents/mandelkern_report.pdf>

Matwyshyn, Andrea M., 'Data Devolution: Corporate Information Security, Consumers and the Future of Regulation' (2010) 84 *Chicago-Kent Law Review* 22

Matwyshyn, Andrea M., *Harboring Data: Information Security, Law, and the Corporation* (Stanford Law Books 2009)

Matwyshyn, Andrea M., 'Material Vulnerabilities: Data Privacy, Coroprate Information Security and Securities Regulation' (2005) 3 *Berkeley Business Law Journal* 66

Maurushat, A., 'Data Breach Notification Law Across the World from California to Australia' (Working Paper, 2009)

Justice Maxwell, Chris, 'Is the giving of reasons for administrative decisions a question of natural justice?' (2013) 20 *AJ Admin L* 76

McCullagh, Karen, 'Protecting ‘privacy’ through control of ‘personal’ data processing: A flawed approach' (2009) 23(1-2) *International Review of Law, Computers & Technology* 13

Meints, Martin 'The Relationship between Data Protection Legislation and Information Security Related Standards' in Vashek Matyáš et al (eds), *The Future of Identity in the Information Society: IFIP Advances in Information and Communication Technology* (Springer Boston, 2009).

Miers, Andrew and Elise Martin, ‘Lessons from recent data breaches’ (2012) (9) 2 Privacy Law Bulletin 24

Mitrakas, Andreas, 'Assessing liability arising from information security breaches in data privacy' (2011) 1(2) (May 1, 2011) *International Data Privacy Law* 129.

Möller, Sebastian et al, 'Modeling the behavior of users who are confronted with security mechanisms' (2011) 30(4) *Computers & Security* 242

Moore, T. and R. Anderson, 'Internet Security' in M. Peitz and J Waldfogel (eds), *The Oxford Handbook of the Digital Economy* ( Oxford University Press, 2011)

Mulligan, D and J King, 'Bridging the Gap Between Privacy and Design' (14) 4 Journal of Constitutional Law 989

Needles, S A ‘The Data Game: Learning to Love the State-Based Approach to Data Breach Notification Law’ (2009) 88 *N.C.L. Rev* 267.

Nehf, James P., 'Recognizing the Societal Value in Information Privacy' 78 *Wash. L. Rev.*

Nielsen, Vibeke Lehmann and Christine Parker, 'Testing Responsive Regulation in Regulatory Enforcement' (2009) 3(4) *Regulation and Governance*

Nissenbaum, Helen, 'Where Computer Security Meets National Security' (2005) 7(2) *Ethics and Information Technology*.

O’Connor, K., ‘The Federal Privacy Commissioner: pursuing a systemic approach' (2001) 7(1) *University of New South Wales Law Journal Forum* 13

Office of the Information Commissioner Canada, *Ensuring operational integrity and corporate support for investigations* < http://www.oic-ci.gc.ca/eng/annual-reports-rapports-annuel_2012-2013_9.aspx>

Open Security Foundation, *DataLoss DB* <http://datalossdb.org/>

Organisation for Economic Cooperation and Development, *Guidelines Covering the Protection of Privacy and Transborder Data Flows of Personal Data* adopted by the OECD Council on 23 Sept.1980 (OECD Doc. C(80)58/Final)

Organisation for Economic Co-operation and Development, *Explanatory Memorandum Guidelines Covering the Protection of Privacy and Transborder Data Flows of Personal Data*, <http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm#memorandum>

Organisation for Economic Co-operation and Development *OECD Guidelines for the Security of Information Systems and Networks* Recommendation of the OECD Council at its 22nd Session on 14 – 15 October 1992 (OECD, 1992) <http://www.oecd.org/internet/ieconomy/oecdguidelinesforthesecurityofinformationsystems1992.htm>

Organisation for Economic Co-operation and Development, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* Recommendation of the OECD Council at its 1037th Session on 25 July 2002 <http://www.oecd.org/internet/interneteconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm>

Organisation for Economic Cooperation and Development, *The Role of the 2002 Guidelines: Towards Cybersecurity for an Open and Interconnected Economy* (OECD Digital Economy Papers No 209, OECD Publishing, 2012 ) <http://dx.doi.org/10.1787/5k8zq930xr5j-en>.

Organisation for Economic Co-operation and Development, *Review of the 2002 Guidelines* (OCED, 2012) <http://www.oecd.org/sti/ieconomy/Security%20guidelines%20review.pdf>

Osterhage, Wolfgang *Wireless Security* (Science Publishers, 1st ed, 2011)

Panko, R. R., *Corporate computer and network security* (Pearson Prentice Hall, 2004)

Parker, C., 'Reinventing Regulation within the Corporation: Compliance Oriented Regulatory Innovation' (2000) 32 *Administration and Society* 29

Parker, C., 'Twenty years of responsive regulation: An appreciation and appraisal' (2013) 7 *Regulation & Governance* 2.

Parker, C. and Vibeke Lehmann Nielsen, *Explaining Compliance: Business Responses to Regulation* (Edward Elgar Publishing, 2011).

Parker, Donn, 'Making the Case for Replacing Risk-Based Security' in C Warren Axelrod, Jennifer Bayuk and Daniel Schutzer (eds), *Enterprise Information Security and Privacy* (Artech House Books, 2009)

Parliament of Australia, Senate Legal and Constitutional References Committee, 'The Real Big Brother: Inquiry into the *Privacy Act* 1988' (2005)

Parliament of Australia, Senate Legal and Constitutional Affairs Legislation Committee, 'Privacy Amendments (Privacy Alerts) Bill 2013' (2013)

Parliament of Australia, Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, Estimates Hearing Budget Supplementary (18 November 2013)

Parliament of Australia, Senate Legal and Constitutional Affairs Legislation Subcommittee, Parliament of Australia, *Estimates Hearing* (14 February, 2012)

Patterson, Dennis (ed), *A Companion to Philosophy of Law and Legal Theory* (Wiley-Blackwell, 2010)

Peltier, T 'Establishing business control for electronic mail communications' (1998) 12 *Information Systems Security* 34

Picanso, Kathryn, 'Protecting Information Security Under a Uniform Data Breach Notification Law' (2006) 75 (1) *Fordham Law Review* 355.

Poole, Vernon, 'IT Governance Metrics, Measurements and Benchmarking Global E-Security' in Hamid Jahankhani, Kenneth Revett and Dominic Palmer-Brown (eds), *Communications in Computer and Information Science* (Springer Berlin Heidelberg, 2008)

Powell, Connie Davis 'You Already Have Zero Privacy, Get over It - Would Warren and Brandeis Argue for Privacy for Social Networking; ' (2011) 31 *Pace L. Rev.* 147

Privacy Clearing House, *Chronology of Data Breaches. Security Breaches 2005 - Present* <http://www.privacyrights.org/data-breach>

Privacy Commissioner of Canada, 'Leading by Example: Key Developments in the First Seven Years of the Personal Information Protection and Electronic Documents Act (PIPEDA)' (Office of the Privacy Commissioner of Canada, 2008).

Radke, Kenneth '"Who decides?": security and privacy in the wild'(Paper presented at the 25th Australian Computer-Human Interaction Conference: Augmentation, Application, Innovation, Collaboration, 2013).

Ragan, Charles R., 'Information Governance: It's a Duty and It's Smart Business' (2013) 19 *Richmond Journal of Law and Technology*

Raz, J, 'Legal Principles and the Limits of Laws' (1977) 81 *Yale Law Journal* 823

Raggad, Bel G., *Information Security Management Concepts and Practice* (CRC Press, 2010).

Reed, Chris and John Angel, *Computer law : the law and regulation of information technology* (Oxford University Press, 6th ed, 2007)

Regan, Priscilla, 'Privacy and Commercial Use of Personal Data: Policy Developments in the United States' (2003) 11(1) *Journal of Contingencies and Crisis Management* 1.

Regan, Priscilla M., 'Legislating Privacy: Technology, Social Values and Public Policy' (1995)

Reidenberg, Joel R, 'Privacy Wrongs in Search of Remedies' 54 *Hastings L.J.*

Report of the Committee on Privacy, Cmnd. 5012, HMSO,1972.

Report on the Committee of Data Protection (1978) Cmnd 7341

Rhee, Hyeun-Suk, Young U. Ryu and Cheong-Tag Kim, 'Unrealistic optimism on information security management' (2012) 31(2) *Computers & Security* 221

Robinson, Neil et al, 'Review of the European Data Protection Directive' (RAND Corporation, 2009)

Romanosky S, D A Hoffman, and A Acquisti, 'Empirical Analysis of Data Breach Litigation' (2014) 11(1) *Journal of Empirical Legal Studies* 74

Romanosky, S, R Telang, and A Acquisti, 'Do Data Breach Disclosure Laws Reduce Identity Theft?' (2011) 30(2) *Journal of Policy Analysis and Management* 256

Rotenberg, Marc, 'Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)' (2011) 1 *Stan. Tech. L. Rev.* 1.

Rowlingson, Robert and Richard Winsborrow, 'A comparison of the Payment Card Industry data security standard with ISO17799' (2006) 2006(3) *Computer Fraud & Security* 16

Rule, James B. and Graham Greenleaf, *Global Privacy Protection* (Edward Elgar Publishing, 2008)

Russell, G. and T. Gangemi, *Computer security basics* (O'Reilly & Associates, Inc, 1991)

Saurwein, F, 'Regulatory choice for alternative modes of regulation: How context matters' (2011) 33(3) *Law and Policy* 22

Schneider, J W 'Preventing Data Breaches: Alternative Approaches to Deter Negligent Handling of Consumer Data' (2009) 15 *Boston University Journal of Science & Technology Law* 25

Schutz, Philip, 'Accountability and Independence of Data Protection Authorities - A Trade Off?' in Daniel Guagnin et al (eds), *Managing Privacy through Accountability* (Palgrave Macmillan, 2012)

Schwarcz, Steven L., 'The 'Principles' Paradox' (2009) 10(2) *European Business Organization Law Review* 175

Schwartz, Paul M. and Edward Janger, 'Notification of Data Security Breaches' (2007) 105 *Michigan Law Review* 913.

Schwartz, Paul M., 'The EU-US Privacy Collision: A Turn to Institutions and Procedures' (May 2013) 126 *Harvard Law Review*

Scott, Michael D. 'The FTC, The Unfairness Doctrine, and Data Security Breach Litigation: Has the Commission Gone Too Far?' (2008) 60 *Admin. L. Rev 129.*

Serwin, Andrew, 'The Federal Trade Commission and Privacy: Defining Enforcement and Encouraging the Adoption ofBest Practices' (2011) 48 *San Diego L. Rev* 809.

Siegel, Kenneth M., 'Protecting the Most Valuable Corporate Asset: The Electronic Data, Identity Theft, Personal Information and the Role of Data Security in the Information Age ' (2007) 111 *Penn State Law Review*

Siponen, Mikko and Harri Oinas-Kukkonen, 'A Review of Information Security Issues and Respective Research Contributions' (2007) 38(1) *The Database for Advances in Information Systems* 60

Siponen, Mikko and Robert Willison, 'Information security management standards: Problems and solutions' (2009) 46(5) *Information & Management* 267

Siponen, Mikko T., 'An analysis of the traditional IS security approaches: implications for research and practice' (2005) 14(3) *European Journal of Information Systems* 303

Smedinghoff, Thomas J, Information Security Law: The Emerging Standard for Corporate Compliance (IT Governance Publishing, 2008)

Smedinghoff, Thomas J, 'Legal and Regulatory Obligations' in C Warren Axelrod, Jennifer Bayuk and Daniel Schutzer (eds), Enterprise Information Security and Privacy (Artech House Books, 2009) 258

Smedinghoff, Thomas J, 'The State of Information Security Law' (2008) <http://ssrn.com/abstract=1114246>

Smyth, Sara M, 'Does Australia Really Need Data Breach Notification Laws - And If So, What Kind' (2012-2103) 22(2) *Journal of Law, Information and Science 159*

Solove, Daniel, 'Introduction: Privacy Self-Management and the Consent Dilemma 1' (May 2013) 126 *HVLR* 20

Solove, Daniel, 'Conceptualizing Privacy' (July 2002) 90(5) *California Law Review*

Solove, Daniel, 'A Taxonomy of Privacy' (2006) 154(3) *University of Pennsylvania Law Review*

Standards Australia, 'OAIC Consultation Submission: Guide to Information Security: 'Reasonable steps' to protect personal information' 4 January 2013 <

http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security-reasonable-steps-to-protect-personal-information-consultation>

Steve, Tombs, 'Understanding Regulation' (2002) 11(1) *Social and Legal Studies* 113

Strachan, Jane, 'Cybersecurity Obligations' (2005) 20 *Maine Bar Journal* 90

Sundt, Chris, 'Information security and the law' (2006) 11(1) *Information Security Technical Report* 2

Sunstein, C. and R. Thaler, *Nudge* (New Haven, 2008)

Susanto, H, M Nabil Almunawar and Yong Chee Tuan, 'Information Security Management System Standards: A Comparative Study of the Big Five' (2011) 11 *International Journal of Electrical and Computer Sciences* 23

Thaw, David, 'Comparing Management-Based Regulation and Prescriptive Legislation: How to Improve Information Security Through Regulation' (May 2013)

Timson, Lia 'Thousands of domain registrar's customer details exposed' (December 23, 201 ) *The Sydney Morning Herald (online)* <http://www.smh.com.au/it-pro/security-it/thousands-of-domain-registrars-customer-details-exposed-20111223-1p8us.html>

The Rand Corporation, *Rand Report R-609*, *Security Controls for Computer Systems* (Department of Defense, February 1970) <http://www.rand.org/pubs/reports/R609-1/index2.html>.

Thompson, Paul 'Privacy, Secrecy and Security' (2001) 3(3) *Ethics and Information Technology* 13

Thornton, Dorothy, Neil A. Gunningham and Robert A. Kagan, 'General Deterrence and Corporate Environmental Behavior' (2005) 27(2) *Law & Policy* 262

Tipton, Harold F. and Micki Krause, *Information Security Management Handbook* (EBooks Corporation, 2007)

Tsacalos, Ashley and Vanessa Verzi, 'Civil penalties for breach of privacy — coming soon! ' (2013) 10(2) *Privacy Law Bulletin* 28.

Tsohou, Aggeliki et al, 'A security standards' framework to facilitate best practices' awareness and conformity' (2010) 18(5) *Information Management & Computer Security* 350

United States Department of Health, Education and Welfare ‘Records, Computers and the Rights of Citizens, Report of the U.S. Secretary of Health,

Education and Welfare's Advisory Committee on Automated Personal Data Systems,' (July, 1973)

van Biene-Hershey, Margaret 'IT Security and IT Audting Betwen 1960 and 2000' in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007)

Vance, Anthony, Mikko Siponen and Seppo Pahnila, 'Motivating IS security compliance: Insights from Habit and Protection Motivation Theory' (2012) 49(3–4) *Information & Management* 190

Varian, Hal R., 'Managing Online Security Risks' (2000) *New York Times; New York, N.Y.;*

von Solms, Basie, 'Information Security governance: COBIT or ISO 17799 or both?' (2005) 24(2) *Computers & Security* 99

von Solms, Rossouw, 'Information Security Management (1): why information security is so important' (1998) 6(4) *Information Management & Computer Security* 174

von Solms, Rossouw, 'Information Security Management: Why Standards are Important' (1999) 7(1) *Information Management & Computer Security* 50

Waters, Nigel, 'Interpreting the Security Principle' (Paper presented at Symposium: Interpreting Privacy Principles: Chaos or Consistency?', Sydney, 17 May 2006)

Waters, Nigel , Graham Greenleaf and Paul Roth, *IPPs examined: The Security Principle v.6* (Working Paper No 1, Cyberspace Law and Policy Centre, University of New South Wales, March 2007 <http://www.cyberlawcentre.org/ipp/publications.html>.

Waters, Nigel and Graham Greenleaf, 'IPPs examined: The Security Principle' (2004) 11(3) *Privacy Law & Policy Reporter*

Waters, Nigel, Abi Paramaguru and Anna Johnston, 'Enforcement of privacy laws – issues arising from Australian experience v.2' (Working Paper No 3, Cyberspace Law & Policy Centre, UNSW, November 2007)

Verizon Ltd, 'Data Breach Investigation Report' (2014)

Justice Weinberg, Mark *Adequate, Sufficient and Excessive Reasons* (Judicial College of Victoria, 2014).

Werlinger, R, K Hawkey and K Beznosov, 'An integrated view of human, organizational, and technological challenges of IT security management' (2009) 17(1) *Information Management & Computer Security* 4

White, Daniel M., 'The Federal Information Security Management Act o 2002: A Potemkin Village' (2010) 79 *Fordham Law Review*

Wilson, Nigel, 'Regulating the information age — How will we cope with technological change?' (2010) 33 *Aust Bar Rev*

Winn, Jane, 'Are "Better" Security Breach Notification Laws Possible?' (2009) 24 *Berkeley Tech. L.J.*

Withnall, Sarah and Michelle Evans, *Administrative Law* (LexisNexis Butterworths, 2010).

Witzleb, Normann, 'Privacy law for the 21st century: Key aspects of the Australian Law Reform Commission review' (2007) 35 *ABLR*

Wong, Rebecca 'The Data Protection Directive 95/46/EC: Idealisms and realisms' (2012) 26(2-3) *International Review of Law, Computers & Technology* 229

Woulds, John 'Information privacy and security - A regulator's priorities' (1997) 2(1) *Information Security Technical Report* 38

Yost, Jeffrey R., 'A History of Computer Security Standards' in Karl de Leeuw, Maria Michael and Jan Bergstra (eds), *The History of Information Security: A Comprehensive Handbook* (Elsevier, 2007)

Yu, Peter K., 'The Political Economy of Data Protection' (2009) 84 *Chicago-Kent Law Review*

UK Information Commissioner's Office, 'Data Protection Act 1988 Monetary Penalty Notice Dated: 14 January 2013 Name: Sony Computer Entertainment Europe Limited' < http://ico.org.uk/~/media/documents/library/Data_Protection/Notices/sony_monetary_penalty_notice.ashx>

UK Information Commissioners Office 'Consumer advice following ebay 'hack"' <http://ico.org.uk/news/current_topics/ebay-hack-consumer-advice>

UK Information Commissioner's Office,' Looking Ahead Staying Ahead: Towards a 2020 Vision for Information Rights' <http://www.ico.org.uk/about_us/consultations/our_consultations>

**OAIC and OPC Publications**

**Annual reports**

Office of the Privacy Commissioner, 'Operation of the Privacy Act Annual Report 1 July 2009 -30 June 2010' (2010)

Office of the Australian Information Commissioner, 'Annual Report 2010 - 2011' (2011) <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201011/>

Office of the Australian Information Commissioner 'Annual Report 2011 - 2012' (2102) <http://www.oaic.gov.au/about-us/corporate-information/annual-reports/oaic-annual-report-201112/>

Office of the Australian Information Commissioner, 'Annual Report 2012 - 2013' (2013) <http://www.oaic.gov.au/images/documents/about-us/corporate-information/annual-reports/Annual-report-2012-13/Complete_pdf_AR_2012-13.pdf>

Office of the Australian Information Commissioner 'Quarterly statistics: April–June 2014' <http://www.oaic.gov.au/about-us/corporate-information/budget-and-statistics/quarterly-statistics-april-june-2014>

**Audit reports**

Office of the Australian Information Commissioner, 'ACT Education and Training Directorate: Final audit report (Information Privacy Principles audit)' (December 2013) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/collection-and-requests-for-student-information>

Office of the Australian Information Commissioner, 'Australian Federal Police (ACT Policing Branch) Audit Report' (July 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/australian-federal-police-act-policing-branch-audit-report>

Office of the Australian Information Commissioner,'Collection and security of student personal information – Canberra Institute of Technology: Audit Report' (April 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/collection-and-security-of-student-personal-information-canberra-institute-of-technology-cit>

Office of the Australian Information Commissioner, 'Healthcare Identifiers Service: Audit report' (June 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/healthcare-identifiers-service-audit-report>

Office of the Australian Information Commissioner 'National Document Verification Service, Centrelink - Audit Report' (June 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/national-document-verification-service-centrelink-audit-report>

Office of the Australian Information Commissioner, 'National Document Verification Service - Department of Foreign Affairs and Trade - Audit Report 2012' (December 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/national-document-verification-service-department-of-foreign-affairs-and-trade-audit-report-2012>

Office of the Privacy Commissioner, 'Passenger Name Records (PNR data) Audit Report No 1' (December 2009)

Office of the Privacy Commissioner, 'Passenger Name Records (PNR data) Audit Report No 2' (January 2010).

Office of the Australian Information Commissioner ‘Passenger Name Records (PNR data) Australian Customs and Border Protection Service Audit Report’ (July 2013)

Office of the Australian Information Commissioner ‘Public Transport Systems: MyWay audit’ June 2013 < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/public-transport-systems-myway-audit#part3-issues>

Office of the Australian Information Commissioner, ‘Requests for Information for Passenger-Name Records Data – Australian Customs and Border Protection Service Audit Report’ (June 2013) < http://www.oaic.gov.au/privacy/applying-privacy-law/list-of-privacy-assessments/requests-for-information-for-passenger-name-record-data-australian-customs-and-border-protection-service-audit-report>

**Guides, guidelines, information sheets and fact sheets**

Office of the Australian Information Commissioner, 'Australian Privacy Principles Guidelines' (2014)

Office of the Australian Information Commissioner, 'Data Breach Notification: A guide to handling personal information security breaches ' (April 2012) <http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html>

Office of the Australian Information Commissioner, ‘Guide to developing an APP privacy policy’ (May 2014) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-developing-an-app-privacy-policy>

Office of the Australian Information Commissioner, ‘Guide to Information Security: reasonable steps to protect personal information’ (April 2013) <http://www.oaic.gov.au/privacy/privacy-resourcces/privacy-guides/guide-to-information-security>

Office of the Australian Information Commissioner ‘Guide to information security Consultation draft – December 2012’ < http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security>

Office of the Australian Information Commissioner, 'Guide to Producing Case Notes' (January 2013) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/guide-to-producing-case-notes>

Office of the Australian Information Commissioner, ‘Guide to undertaking privacy impact assessments (May 2014) ‘< http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guide-to-undertaking-privacy-impact-assessments>

Office of the Australian Information Commissioner, 'Privacy Complaints and Procedures Manual' <http://www.oaic.gov.au/about-us/corporate-

information/privacy-operational/privacy-complaints-practice-and-procedure-manual/file-management-and-security-standards>

Office of the Australian Information Commissioner, 'Privacy Fact Sheet 7: Ten Steps to protect other people's personal information' (April 2012) <http://www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet7_10steps_protect_personal_info.html>

Office of the Australian Information Commissioner, 'Privacy Fact Sheet 8: Ten Steps to protect your personal information ' (April 2012) <http://www.oaic.gov.au/publications/privacy_fact_sheets/privacy_fact_sheet8_10steps_protect_your_information.html>.

Office of the Australian Information Commissioner, "Privacy Fact Sheet 10: What will happen to my complaint" (June 2012)

Office of the Australian Information Commissioner, 'Privacy fact sheet 11: How will the OAIC handle a privacy complaint against my organisation? ' (June 2012)

Office of the Australian Information Commissioner, 'Privacy fact sheet 12: Conciliation of privacy complaints ' (June 2012) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-12-conciliation-of-privacy-complaints>

Office of the Privacy Commissioner, ' Information Sheet (Private Sector) 30 - 2010: ID scanning in clubs and pubs' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/information-sheet-private-sector-30-2010-id-scanning-in-clubs-and-pubs>.

Office of the Australian Information Commissioner, 'Privacy Impact Assessment Guide Reviewed May 2010' <http://www.privacy.gov.au/materials/types/guidelines/view/6590>

Office of the Australian Information Commissioner, *Privacy Performance Assessment Manual* (2012) <http://www.oaic.gov.au/about-us/corporate-information/privacy-operational/privacy-performance-assessment-manual>.

Office of the Australian Information Commissioner, 'Privacy Regulatory Action Policy (draft)' (March 2014) <http://www.oaic.gov.au/news/consultations.html#info_security>

Office of the Federal Privacy Commissioner, 'About the Office Information Sheet - Conciliation of Privacy Complaints' (February 2008)

Office of the Federal Privacy Commissioner, 'Australian Privacy Principles Companion Guide' (2010)

Office of the Federal Privacy Commissioner, 'Getting in on the Act: Review of the Private Sector Provisions of the Privacy Act 1988 ' (March 2005) <http://www.oaic.gov.au/images/documents/migrated/migrated/revreport.pdf>

Office of the Federal Privacy Commissioner, 'Guidelines to the National Privacy Principles' (2001) <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/guidelines-to-the-national-privacy-principles>

Office of the Federal Privacy Commissioner, 'Information Sheet (Private Sector) 6 – Security and Personal Information' (2001)

Office of the Federal Privacy Commissioner, *Plain English Guidelines to Information Privacy Principles* (October 1994) <http://www.oaic.gov.au/images/documents/migrated/migrated/HRC_PRIVACY_PUBLICATION.pdf_file.p6_4_14.4.pdf>

Office of the Federal Privacy Commissioner, 'Private Sector Information Sheet 13 - The Privacy Commissioner's Approach To Promoting Compliance With The Privacy Act' December 2001

Office of the Federal Privacy Commissioner, 'Public Sector Information Sheet 2 - A step by step guide to internal investigations of privacy complaints by Australian and ACT government agencies' (August 2008)

**OMI reports**

Office of the Australian Information Commissioner, *Own Motion Investigation Report – Vodafone Hutchison Australia* (February 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/vodafone-hutchison-australia>.

Office of the Australian Information Commissioner, *Telstra Corporation Limited Own Motion Investigation* (7 July 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited-telstra>

Office of the Australian Information Commissioner, *Sony PlayStation Network/Qriocity Own Motion Investigation* (29 September 2011) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/sony-playstation-network-qriocity>

Office of the Australian Information Commissioner, *Dell Australia and Epsilon Own Motion Investigation Report* (July 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-omi-reports/dell-australia-and-epsilon#_Toc330548364>

Office of the Australian Information Commissioner, *Telstra Corporation Limited: Own Motion Investigation* (July 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-corporation-limited>

Office of the Australian Information Commissioner, *Medvet Science Pty Ltd Own Motion Investigation* (July 2012) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/medvet-science-pty-ltd-own-motion-investigation-report>

Office of the Australian Information Commissioner, *Professional Service Revew Agency: Own Motion Investigation* (15 December 2011) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/professional-services-review-agency>

Office of the Australian Information Commissioner, *First State Super Trustee Corporation: Own Motion Investigation Report* (June 2012) < http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-omi-reports/first-state-super-trustee-corporation-own-motion-investigation-report>

Office of the Australian Privacy Commissioner, Telstra Corporation Limited: Own Motion Investigation (March 2014) <http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/telstra-omi-march-2014>

**Statements, media releases and presentations**

McMillan, John; James Popple and Timothy Pilgrim, 'Australian Government's Budget decision to disband OAIC' (Statement, 13 May 2014) <http://www.oaic.gov.au/news-and-events/statements/australian-governments-budget-decision-to-disband-oaic/australian-government-s-budget-decision-to-disband-oaic>.

Office of the Australian Information Commissioner, 'AFP data breach', (Statement, 28 August 2014) < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/afp-data-breach/>

Office of the Australian Information Commissioner, 'ACCC data breach' (Statement, 11 April 2014) < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/accc-data-breach/accc-data-breach>

Office of the Australian Information Commissioner, 'Australian Privacy Commissioner concludes Sony investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation>

Office of the Australian Information Commissioner, 'eBay data breach'(Statement, 22 May 2014) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/ebay-data-breach/ebay-data-breach>

Office of the Australian Information Commissioner, 'Heartbleed bug' (Statement, 11 April 2014) < http://www.oaic.gov.au/news-and-events/statements/privacy-statements/heartbleed-bug/heartbleed-bug>

Office of the Australian Information Commissioner, 'Privacy Commissioner Releases Investigation Findings' (Media Release, 16 February 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-releases-vodafone-findings>

Office of the Australian Information Commissioner, 'Privacy Commissioner: Website privacy policies are too long and complex' (Media Release, 14 August

2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-website-privacy-policies-are-too-long-and-complex>.

Office of the Australian Information Commissioner, 'The OAIC's enforcement approach to new privacy laws from 12 March 2014' Statement from the Australian Information Commissioner and Privacy Commissioner, 28 February 2014 http://www.oaic.gov.au/news-and-events/statements/privacy-statements/the-oaics-enforcement-approach-to-new-privacy-laws-from-12-march-2014/the-oaic-s-enforcement-approach-to-new-privacy-laws-from-12-march-2014-statement-fro

Office of the Australian Information Commissioner, 'Take time to protect your privacy during Cyber Security Awareness Week' (Media Release, 20 May 2013) < http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/take-time-to-protect-your-privacy-during-cyber-security-awareness-week>.

Office of the Australian Information Commissioner, 'Telstra Breaches Privacy Act' (Media Release, 29 June 2012) <http://www.oaic.gov.au/news/media_releases/media_release_120629_telstra_breaches_privacy_act.html>

Timothy Pilgrim, Australian Privacy Commissioner "ANZ e-statement – Statement from Australian Privacy Commissioner, Timothy Pilgrim: update" (Statement, XXX)<http://www.oaic.gov.au/news-and-events/statements/privacy-statements/anz-e-statement-data-breach/anz-e-statement-statement-from-australian-privacy-commissioner-timothy-pilgrim-update>

Timothy Pilgrim, Australian Privacy Commissioner, 'Australians better protected with mandatory data breach notification' (Media Release, 28 May 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australians-better-protected-with-mandatory-data-breach-notification>

Timothy Pilgrim, Australian Privacy Commissioner, 'Australian Privacy Commissioner concludes Sony investigation' (Media Release, 29 September 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/australian-privacy-commissioner-concludes-sony-investigation

Timothy Pilgrim, Australian Privacy Commissioner 'Information security is now the major issue affecting consumer privacy' (Media Release, 29 May, 2013) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/information-security-is-now-the-major-issue-affecting-consumer-privacy>

Timothy Pilgrim, Australian Privacy Commissioner, "Investigation into Sony data breach Statement from Australian Privacy Commissioner" (Statement, 4 May 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-

statements/sony-playstation-network/investigation-into-sony-data-breach-4-may-2011>

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy Commissioner responds to media claims about Medvet investigation – Letter to the editor of The Australian newspaper from Australian Privacy Commissioner, Timothy Pilgrim' (Statement, 26 July 2012) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/medvet-investigation/privacy-commissioner-responds-to-media-claims-about-medvet-investigation>

Timothy Pilgrim, Australian Privacy Commissioner, 'Mapping data breach notification' (Presentation at iappANZ data breach panel discussion, Sydney, 6 May 2014 <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/>

Timothy Pilgrim Australian Privacy Commissioner, 'OAIC finalises investigation into Telstra mailing list error' (Media Release, 11 October 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/oaic-finalises-investigation-into-telstra-mailing-list-error>

Timothy Pilgrim Australian Privacy Commissioner, 'Privacy Awareness Week 2013 Privacy Commissioner's Update' (Presentation to Privacy Awareness Week 2013 Business Breakfast, Sydney, 29 April 2013) < http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-awareness-week-privacy-commissioner-s-update>.

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy Commissioner opens investigation into Telstra customer accounts data breach' (Statement, 12 December, 2011) <http://www.oaic.gov.au/news-and-events/statements/privacy-statements/telstra-data-breach/>

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy Commissioner releases Vodafone Findings' (Media Release, 16 February 2011) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/privacy-commissioner-releases-vodafone-findings>

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy law reform: challenges and opportunities', (Presentation to Emerging Challenges in Privacy Law Conference, 23 February 2012) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-law-reform-challenges-and-opportunities>

Timothy Pilgrim, Australian Privacy Commissioner, "Privacy law reform — Get in on the Act" (Presentation at the iappANZ Privacy Awareness Week seminar, Brisbane, 1 May 2013) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-law-reform-get-in-on-the-act>

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy Reform - Act Three' (Presentation to the iappANZ 'Privacy Unbound' summit, Sydney, 25 November 2013) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-reform-act-three>

Timothy Pilgrim, Australian Privacy Commissioner, 'Privacy and Transparency'(Presentation to the Privacy Awareness Week 'Up close and personal' business breakfast, 5 May 2014) <http://www.oaic.gov.au/news-and-events/speeches/privacy-speeches/privacy-and-transparency>

Timothy Pilgrim, Australian Privacy Commissioner, 'Telstra breaches *Privacy Act*' (Media Release, 29 June 2012) <http://www.oaic.gov.au/news-and-events/media-releases/privacy-media-releases/telstra-breaches-privacy-act>.

Timothy Pilgrim, Australian Privacy Commissioner, 'Update your privacy setting' (Presentation by to the Communications and Media Law Association, Sydney, 7 March 2013)

**Internet materials**

'OAICgov' https://twitter.com/OAICgov.

<http://www.youtube.com/user/OAICgov>.

<https://www.facebook.com/OAICgov>

Office of the Australian Information Commissioner 'Advisory Privacy Guidelines' < http://www.oaic.gov.au/privacy/applying-privacy-law/advisory-privacy-guidelines/>

Office of the Australian Information Commissioner, 'Applying Privacy Law' (1 September 2014) < http://www.oaic.gov.au/privacy/privacy-act/applying-privacy-law>.

Office of the Australian Information Commissioner, 'Audit Report' (2 July 2014) < http://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/ >.

Office of the Australian Information Commissioner, 'Commissioner Initiated Investigation Reports (30 June 2014) < http://www.oaic.gov.au/privacy/applying-privacy-law/commissioner-initiated-investigation-reports/>.

Office of the Australian Information Commissioner, *Our Structure* (March 2013) < http://www.oaic.gov.au/about-us/who-we-are/our-structure/>

Office of the Australian Information Commissioner, 'Privacy Agency Resources' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-agency-resources/>

Office of the Australian Information Commissioner, 'Privacy Business Resources' <http://www.oaic.gov.au/privacy/privacy-resources/privacy-business-resources/?

Office of the Australian Information Commissioner, 'Privacy case notes' (12 April 2013) <http://www.oaic.gov.au/privacy/applying-privacy-law/privacy-case-notes>.

Office of the Australian Information Commissioner 'Privacy Fact Sheets' http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/.

Office of the Australian Information Commissioner 'Privacy Guides' < http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/>

Office of the Australian Information Commissioner 'Privacy Submissions' (30 June 2014) < http://www.oaic.gov.au/news-and-events/submissions/privacy-submissions/>

Office of the Australian Information Commissioner, "Stay Smart Online", OAIC Homepage (3 June 2014) <http://www.oaic.gov.au/>

**Submissions to the OAIC**

Australian Information Security Association, 'The AISA Response to the Office of the Australian Information Commissioner's Guide to information security Discussion Paper' (7 January 2013)

Email from Glenn Archer to Dimitrios Kormas dated 21 January 2013 <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/AGIMO_response_draft_Information_security_guide.txt>)

Email from Michael Morgan to OAIC, 14 January 2013 at <http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/McAfee_response_draft_Information_security_guide.txt>

Letter from Lockstep Consultant to Ms Angelene Falk, Acting Assistant Commissioner Compliance, 8 January 2013 < http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/Lockstep_response_draft_Information_security_guide.pdf>.

National Archives of Australia, 'Comments on Draft Guide to Information Security' http://www.oaic.gov.au/privacy/privacy-engaging-with-you/previous-privacy-consultations/guide-to-information-security-december-2012/guide-to-information-security-reasonable-steps-to-protect-personal-information-consultation.

NEHTA 'Submission to the Office of the Australian Information Commissioner' 8 January 2013 at < http://www.oaic.gov.au/images/documents/privacy/engaging-with-you/previous-privacy-consultations/info-security-guide/NeHTA_response_draft_Information_security_guide.pdf>

## Newspaper Articles


AAP 'Massive Telstra bungle a privacy breach', *News.com.au* (online), 27 October 2010 <http://www.news.com.au/business/massive-telstra-bungle-a-privacy-breach/story-e6frfm1i-1225944346111>

AAP, 'Vodafone website exposes customer details', *ZDNet* (online), 9 January 2011 <http://www.zdnet.com.au/vodafone-website-exposes-customer-details-339308437.htm>

Baker, Liana 'Sony PlayStation suffers massive data breach', *Reuters* (online) 26 April 2011 <http://www.reuters.com/article/2011/04/26/us-sony-stoldendata-idUSTRE73P6WB20110426>;

Beeby, Dean 'Budget cuts undermine federal access-to-information system: watchdog', *The Canadian Press* (online), 7 April 2013 <http://www.ctvnews.ca/politics/budget-cuts-undermine-federal-access-to-information-system-watchdog-1.1227794>

Bright, Peter, 'Sony hacked yet again, plaintext passwords, e-mails, DOB posted', Arstechnica (online), June 3, 2011 http://arstechnica.com/tech-policy/news/2011/06/sony-hacked-yet-again-plaintext-passwords-posted.ars

Carstensen, Jared, 'Sony PlayStation Hack: 70 Million Users' Details Stolen', *InfoSec Island* (online) 27 April 2011<http://www.infosecisland.com/blogview/13337-Sony-PlayStation-Hack-70-Million-User-Details-Stolen.html>.

Colley, Andrew 'Privacy Commissioner plans hardline approach to new Act. Talks tough on *Privacy Act* amendments', *itNews* (online), 25 November 2013 <http://www.itnews.com.au/News/365375,privacy-commissioner-plans-hardline-approach-to-new-act.aspx>.

Colley, Andrew 'Privacy Commissioner Timothy Pilgrim will probe Telstra's culture in light of privacy breach', *The Australian (online)* 29 June, 2012 < http://www.theaustralian.com.au/australian-it/telecommunications/privacy-commissioner-timothy-pilgrim-will-probe-telstras-culture-in-light-of-privacy-breach/story-fn4iyzsr-1226412092746>

Cooper, Hayden "Defence under Investigation Over Privacy Breach" *ABC* (online), 6 March, 2012 <http://www.abc.net.au/news/2012-03-05/defence-under-investigation-over-privacy-breach/3870002>

Coyne, Allie and Paris Cowan, 'Immigration dept confirms asylum seeker data breach', *ITNews (online)* 19 February 2014 <http://www.itnews.com.au/News/372741,immigration-dept-admits-asylum-seeker-data-breach.aspx#ixzz366DGFeT>

'Data security expert: Sony knew it was using obsolete software months in advance', *Consumer Reports News* (online), 4 May 2011 <http://www.consumerreports.org/cro/news/2011/05/data-security-expert-sony-knew-it-was-using-obsolete-software-months-in-advance/index.htm>

Dearne, Karen ‘Dell Australia Impacted by Epsilon email breach’, *The Australian IT* (online), 6 April 2011

Dearne, Karen ‘Privacy czar to investigate Epsilon email breach’, *The Australian* (online), 7 April 2011 < http://www.theaustralian.com.au/technology/privacy-czar-to-investigate-epsilon-email-breach/story-e6frgakx-1226035569602#sthash.w4iypq2o.dpuf

Dostal, Erin, 'Report: Online security increasingly important to consumers', *DMNews (online)* March 7, 2012 <http://www.dmnews.com/report-online-security-increasingly-important-to-consumers/article/231065/>

Edwards, Cliff, Karen Gullo, and Michael Riley, ‘Sony Faces Lawsuit, Regulators’ Scrutiny Over PlayStation Breach’ *Bloomberg* (online) 28 April 2011 <http://www.bloomberg.com/news/2011-04-28/sony-faces-lawsuit-regulators-scrutiny-over-playstation-user-data-breach.html>.

Foo, Fran, “Warning after eBay passwords ‘stolen’” *The Australian* (*online*), 23 May 2014 < e6frgakx-1226927542280>

Foo, Fran, 'ACCC admits to data breach, but denies being hacked', *The Australian (online)* 11 April 2014 <http://www.theaustralian.com.au/technology/accc-admits-to-data-breach-but-denies-being-hacked/story-e6frgakx-1226881178192?nk=5a744d7d8b05049d7efbce9a1cf90d69>

Griffith, Chris, 'Australia's Privacy Commissioner Timothy Pilgrim is close to finalising his investigation into April's massive Sony PlayStation hacking and privacy breach', *The Australian (online)* 23 September, 2011

Griffith, Chris and Karen Dearne, ‘Breach sparks security alert: call for laws to protect against Playstation-style attacks’, *The Australian IT* (online), 3 May 2011 <http://www.theaustralian.com.au/australian-it/breach-sparks-security-alert-call-for-laws-to-protect-against-playstation-style-attacks/story-e6frgakx-1226048705602?referrer=email&source=AIT_email_nl&emcmp=Ping&emchn=Newsletter&emlist=Member>

Grubb, Ben 'Long delays before privacy complaints assessed', *The Sydney Morning Herald (online)* 12 September 2013 <http://www.smh.com.au/digital-life/consumer-security/long-delays-before-privacy-complaints-assessed-20130912-2tn72.html#ixzz2yY0zIYho>

Heath, David, 'Lush breach shows Australian privacy laws are a toothless tiger', *IT Wire (online)* 17 February 2011 <http://www.itwire.com/business-it-news/security/45216-lush-breach-shows-australian-privacy-laws-are-a-toothless-tiger?start=1>

“IBM: Companies fail at basic security” *CRN News* (online), 26 September, 2013 <http://www.crn.com.au/News/358316,ibm-companies-fail-at-basic-security.aspx?eid=4&edate=20130926&utm_source=20130926&utm_medium=newsletter&utm_campaign=daily_newsletter>

Jackson, Brian, 'How Not to Get Hacked Lack Sony', *PC World* (online) 7 July 2008 <http://www.pcworld.com/article/148007/security.html>

Kelly, Tim 'Analysis: Sony bungles data breach response', *IT News* (online) 28 April 2011 <http://www.itnews.com.au/News/255788,analysis-sony-bungles-data-breach-response.aspx>.

Krebs, Brian, 'Target: Names, Emails, Phone Numbers on Up To 70 Million Customers Stolen', *KrebsonSecurity (*online*),* 10 January 2014 <http://krebsonsecurity.com/2014/01/target-names-emails-phone-numbers-on-up-to-70-million-customers-stolen/>

O'Brien, Natalie 'Mobile security outrage: private details accessible on net', *The Sydney Morning Herald* (online), 9 January 2011 <http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html#ixzz2hOpjMQ1L>

Ong, Erica 'Sony Pictures says 37,500 customer records exposed' *CNet* (online) 8 June 2011 <http://news.cnet.com/8301-31021_3-20070063-260/sony-pictures-says-37500-customer-records-exposed/>.

Martin, Peter and Lucy Battersby, 'Vodafone may be liable on privacy breach', *The Sydney Morning Herald* (online), 10 January 2011 <http://www.smh.com.au/technology/security/vodafone-may-be-liable-on-privacy-breach-20110109-19jup.html>.

Martin, Sarah 'Investigation into South Australia's Medvet lab after serious privacy breach', *The Advertiser* (online), 18 July 2011 <http://www.news.com.au/national-old/south-australias-medvet-blood-lab-publishes-details-of-paternity-and-drug-test-applicants/story-e6frfkx9-1226096476780

Merritt, C 'Pilgrim has compelling case for conciliated outcomes', *The Australian* (online), 19 August 2011 <http://www.theaustralian.com.au/business/legal-affairs/compelling-case-for-conciliated-outcomes/story-e6frg97x-1226117737294>

Moses, Asher 'Dell Australia customer details stolen in major data breach', *The Sydney Morning Herald* (online), 7 April 2011 <http://www.smh.com.au/technology/security/dell-australia-customer-details-stolen-in-major-global-data-breach-20110407-1d4yd.html#ixzz2gWxiBHkk>

Moses, A, 'Telstra botched mail-out exposes 220,000 customers', *The Sydney Morning Herald* (online), 27 October 2012 <http://www.smh.com.au/technology/security/telstra-botched-mailout-exposes-220000-customers-20101027-173du.html#ixzz2hC0Ak7np>

Moses, Asher 'Paternity and drug test details leak online in privacy breach', *The Sydney Morning Herald* (online) 18 July 2011 <http://www.smh.com.au/technology/security/paternity-and-drug-test-details-leak-online-in-privacy-breach-20110718-1hkyn.html#ixzz2EiZDNyiV>

Moses, Asher and Ben Grubb, 'Telstra Customer database exposed', *The Sydney Morning Herald* (online), 9 December 2011 <http://www.smh.com.au/it-pro/security-it/telstra-customer-database-exposed-20111209-1on60.html>

Moses, Asher 'Vodafone dealer shuts down after expose', *The Sydney Morning Herald* (online) 24 January 2011 <http://www.smh.com.au/technology/technology-news/vodafone-dealer-shuts-down-after-expose-20110124-1a28s.html>

Musil, Steve 'Senator slams Sony's response to security breach', *Cnet* (online), 3 May 2011 <http://www.cnet.com/news/senator-slams-sonys-response-to-security-breach/>

O'Brien, Natalie 'Mobile security outrage: private details accessible on net', *The Sydney Morning Herald* (online), 9 January 2011 <http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html#ixzz2hOpjMQ1L>

'Online medical privacy breach to be probed', *ABC News* (online) 18 July 2011 <http://www.abc.net.au/news/2011-07-18/medvet-privacy-breach-online/2798650>

Parnell, Brid-Aine 'eBay faces Multiple Probes into mega-breach' *The Register* (online), 23 May 2014 <http://www.theregister.co.uk/2014/05/23/ebay_security_breach_investigations/

Pauli, Darren 'Aussie transport system cracked, researchers get free rides ' (October 23, 2012) *Computer Reseller News (online)* <http://www.crn.com.au/News/320290,aussie-transport-system-cracked-researchers-get-free-rides.aspx?eid=4&edate=20121023&utm_source=20121023&utm_medium=newsletter&utm_campaign=daily_newsletter>

Pauli, Darren, "Data breach laws to follow privacy reforms' *ITNews* (online), 4 October 2011 <http://www.itnews.com.au/News/275598,data-breach-laws-to-follow-privacy-reforms.aspx

Pauli, Darren, 'Privacy Commissioner Probes Fairfax Hack', *SC Magazine* 1 February, 2012 <http://www.scmagazine.com.au/News/288847,privacy-commissioner-probes-fairfax-hack.aspx >

Pullar-Strecker, Tom, 'Leaked, Stolen Data Leaps', *The Age (Online)* (New Zealand), December 14 2012 <http://www.theage.com.au/it-pro/security-it/leaked-stolen-data-leaps-by-40-20121214-2bdhm.html>

'Security breach widens at US retailers', *The Australian* (online), 4 April 2011

Simpson, Campbell 'Dell Customer email addresses accessed in Epsilon Breach' *CSO* (online), 6 April 2011

‘Sony bows head over PlayStation security breach’ *The Sydney Morning Herald* (online), 2 May 2011 <http://www.smh.com.au/technology/security/sony-bows-head-over-playstation-security-breach-20110502-1e3m5.html#ixzz2g95KsFNE>

Spiegel, Rob, 'Sony Tallies $171M in Data Breach Losses... and Counting', *Technewsworld (online)* 24 May 2011 <http://www.technewsworld.com/story/72520.html>

Takahashi, Dean, ‘Hacktivist group Anonymous launches “payback” cyber-attack on Sony’, *VB News* (online) 3 April 2011 <http://venturebeat.com/2011/04/03/hacktivist-group-anonymous-launches-payback-cyber-attack-on-sony/>.

Tay, Liz, 'Privacy Commissioner investigates alleged Vodafone breach', *IT News (online),* 10 January 2011 <http://www.itnews.com.au/News/243761,privacy-commissioner-investigates-alleged-vodafone-breach.aspx>

'The 10 Worst Data Breaches of 2013', *ITBusinessEdge (*online*)* <http://www.itbusinessedge.com/slideshows/the-10-worst-data-breaches-of-2013.html>

Thomas, Hedley ‘DNA test names exposed online’, *The Australian* (online), 16 July 2011 < http://www.theaustralian.com.au/news/health-science/dna-test-names-exposed-online/story-e6frg8y6-1226095576596 >.

Thomas, Hedley, ‘Paternity firm slapped over privacy breach’, *The Australian* (online) < http://www.theaustralian.com.au/news/investigations/paternity-firm-slapped-over-privacy-breach/story-fn6tcs23-1226435191069>

Thomas, Hedley, 'Privacy data still online 24 hours after alert ' *The Australian (*online*).*

Thomas, Hedley, '"Rigorous” probe rubber-stamps audit', *The Australian (*online*)* 26 July 2012 <http://www.theaustralian.com.au/national-affairs/opinion/rigorous-probe-rubber-stamps-audit-praising-lab-that-broke-rules/story-e6frgd0x-1226435164479#>

Winterford, Brett ‘Epsilon breach used four-month-old attack’, *ITNews* (online) 7 April 2011 <http://www.itnews.com.au/News/253712,epsilon-breach-used-four-month-old-attack.aspx>.

**CASES**

*A v Australian Information Commissioner* [2011] FCA 520

*‘BO’ v AeroCare Pty Ltd* [2014] AICmr 32

*‘CM’ and Corporation of the Synod of the Diocese of Brisbane* [2014] AICmr 86

*'CP' v Department of Defence* [2014] AICmr 88

*D v Commonwealth Agency* [2010] PrivCmrA 5

*D v Health Service Provider* [2008] PrivCmrA 4.

'D' and Wentworthville Leagues Club [2011] AICmr 9

*E v Financial Institution* [2003] PrivCmrA 3

*E v Retail Organisation* [2007] PrivCmrA 7

*FH v NSW Department of Corrective Services* [2003] NSWADT 72

*G v Counselling Service* [2009] PrivCmrA 9

*H and Registered Club* [2011] AICmrCN 2

*Hammond v Australian Information Commissioner* [2013] FCA 802

*Jones v Office of the Australian Information Commissione*r [2014] FCA 285

*Kawicki v Legal Services Commissioner and Anor* [2002] NSWSC 1072

*M v Commonwealth Agency* [2008] PrivCmrA 13.

*N v Utility Provider* [2006] PrivCmrA 13.

*Own Motion Investigation v Airline* [2009] PrivCmrA 7

*Own Motion Investigation v Information Technology Company* [2010] PrivCmrA 24

*Own Motion Investigation v Medical Centre* [2009] PrivCmrA 6

*Own Motion Investigation v Telecommunications Company* [2010] PrivCmrA 16

*OPC v Bank Institution* [2005] PrivCmrA.

*P and Retail Company* [2011] AICmrCN 10

*Public Service Board (NSW) v Osmond* (1986) 159 CLR 656

*R v Internet Service Provider* [2005] PrivCmrA 17

*S v Health Service Provider* [2008] PrivCmrA 19

*Seven Network (Operations) Limited v Media Entertainment and Arts Alliance* [2004] FCA 637

*'S' and Veda Advantage Information Services and Solutions Limited* [2012] AICmr 33

*Smallbone v NSW Bar Association* [2011] FCA 1145

*V v Health Service Provider* [2006] PrivCmrA 21

*Wijayaweera v Australian Information Commissioner* [2012] FCA 99

## LEGISLATION

### Australian

*Australian Information Commissioner Act 2010* (Cth).

*Data-matching Program (Assistance and Tax) Act 1990* (Cth)

*Freedom of Information Act 1982* (Cth)

*Health Records Act* 2001 (Vic)

*Health Records and Information Privacy Act* 2002 (NSW)

*Information Privacy Act 2009* (Qld)

*Information Privacy Act* 2000 (Vic)

*Information Protection Act* 2002 (NT)

*Personal Information Protection Act* 2004 (Tas)

*Privacy Act 1988* (Cth)

*Privacy Amendment (Enhancing Privacy Protection) Act 2012* (Cth)

*Privacy Amendment (Private Sector) Act 2000* (Cth)

*Privacy Act (Privacy Alerts) Amendment Bill 2013* (Cth)

*Privacy and Personal Information Protection Act* 1997 (NSW)

*Telecommunications Act 1997* (Cth)

### International

Council of Europe Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data, European Treaty Series No. 108; adopted 28 Jan. 1981

European Parliament and Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personla data and on the free movement of such data [1995] OJ L 281/31, art 17.1.

Explanatory Memorandum, 'Privacy Amendment (Enhancing Privacy Protection) Bill 2012'

Gramm-Leach-Bliley Act, Public L. 106-102, Sections 501 and 505(b), 15 U.S.C. Sections 6801, 6805

Health Insurance Portability and Accountability Act, 42 U.S.C. 1320d-2 and 1320d-4 and Final HIPAA Security Regulations, 45 C.F.R. Part 164

Privacy Act of 1974, as amended, codified at 5 U.S.C. § 552a

**OTHER**

Asia Pacific Economic Co-Operation Secretariat, 'APEC Privacy Framework' (2005)

European Commission "Proposal for a Directive of the European and the Council concerning measures to ensure a high common level of network and information security across the Union" SWD(2013)31 final COM (2013) 48 final <http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security>.

Interview with Angelene Falk, Acting Commissioner Compliance, (Sydney, 14 December 2012)

Interview with Timothy Pilgrim, Australian Privacy Commissioner (Sydney, 14 December 20120

NSW Ombudsman, 'Investigating Complaints A manual for investigators' (June 2004) http://www.ombo.nsw.gov.au/news-and-publications/publications/guidelines/state-and-local-government/investigating-complaints-a-manual-for-investigators

U.S. House Energy and Commerce Subcommittee on Commerce, Manufacturing and Trade, 'Hearing on "Sony and Epsilon: Lessons for Data Security Legislation,"' (2 June 2011) <http://democrats.energycommerce.house.gov/index.php?q=hearing/hearing-on-sony-and-epsilon-lessons-for-data-security-legislation-subcommittee-on-commerce-m>

**Standards**

Payment Card Council, 'Payment Card Industry Data Security Standard v3.0' <https://www.pcisecuritystandards.org/security_standards/>.

International Standards Organisation, *ISO/IEC:27001:2013 Information technology – Security techniques – Information security management systems-Requirements* (2013).

International Standards Organisation, ISO/IEC 27002:2013 *Information technology – Security Techniques – Code of Practice for Information Security Management* (2013).

International Standards Organisation, *ISO/IEC 27005: 2008 Information Technology – Security techniques - Information Security Risk Management* (2005)

National Institute of Standards and Technology, 'Glossary of Key Information Security Terms' (2011) <http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf>

National Institute of Standards and Technology, 'Security and Privacy Controls for Federal Information Systems and Organizations (Updated with Errata page May 7, 2013) SP 800-53 Rev. 4 Apr. 2013

**State government security policies**

New South Wales Government, Department of Premier and Cabinet, *M1999-19 Applicability of Memoranda and Circulars to State Owned Corporations*. (NSW Government, 2001).

New South Wales Government, Department of Premier and Cabinet, *MD2012-15 Digitial Informatin Security Policy* (NSW Government, November 2012) < http://www.dpc.nsw.gov.au/__data/assets/pdf_file/0006/146688/Digital_Information_Security_Policy_2012.pdf>

Queensland Government, Chief Information Office, *Queensland Government Information Standard 18: Information Security,* (Department of Science, Information Technology, Innovation and the Arts, December 2012) http://www.qgcio.qld.gov.au/products/qgea-documents/549-information-security/2704-information-security-is18policy.

Victorian Government Chief Technology Advocate, *SEC POL 01 Information Security Management Policy - 2012 version 201* (Victorian Government CIO Council, 1 October 2012) < http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-POL-01-Information-Security-Management-Policy1.pd>.

Victorian Government Chief Technology Advocate, *SEC STD 01 Information Security Management Framework version 3.1* (Victorian Government CIO Council, 1 October 2012) < http://www.digital.vic.gov.au/wp-content/uploads/2014/07/SEC-STD-01-Information-Security-Management-Framework.pdf>.

**Websites**

*A Brief History of Information Security* Lewis University, < http://www.lewisu.edu/academics/msinfosec/history.htm>

'About APRA' (7 January 2014) <http://www.apra.gov.au/AboutAPRA/Pages/Default.aspx>.

About Michael Kirby (October 2014) <http://www.michaelkirby.com.au/index.php?option=com_content&view=article&id=67&Itemid=2>

ARGis Resources, 'Security Principles' < http://resources.arcgis.com/en/communities/enterprise-gis/01n200000030000000.htm>.

C.P. Moore Business Solutions, *About Us* <http://www.cpmoore.com/About_Us.aspx>.

Gilbert, H *Introduction to SNA* (2 February 1995) <http://www.yale.edu/pclt/COMM/SNA.HTM>.

*John W. Mauchly and the Development of the ENIAC Computer* <http://www.library.upenn.edu/exhibits/rbm/mauchly/jwmintro.html >

Moye, William T. 'ENIAC: The Army-Sponsored Revolution' (website) http://ftp.arl.army.mil/~mike/comphist/96summary/.

Medvet Science Pty Ltd, *About Us* <http://www.medvet.com.au/about-us>.

**Other**

Prepared statement of Jeanette Fitzgerald, General Counsel, Epsilon Data Management LLC Before the House Committee on Energy & Commerce, Subcommittee on Commerce, Manufacturing and Trade, U.S. House of Representatives, 2 June 2011

Letter from Kazuo Haria, Chairman, Sony Computer America LLC to Fred Upton Chairman, U.S. House of Representatives, Committee on Energy and Commerce, 'Sony and Epsilon: Lessons for Data Security Legislation', 26 May 2011

WireFire, 'Our Best Ever Cable Broadband Deal' on *Whirlpool Forum* (9 December 2011) <http://forums.whirlpool.net.au/forum-replies.cfm?t=1801978&p=27#r533>